CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE

Threat Evaluation Working Group: Threat Scenarios

February 2020

This page is intentionally left blank.

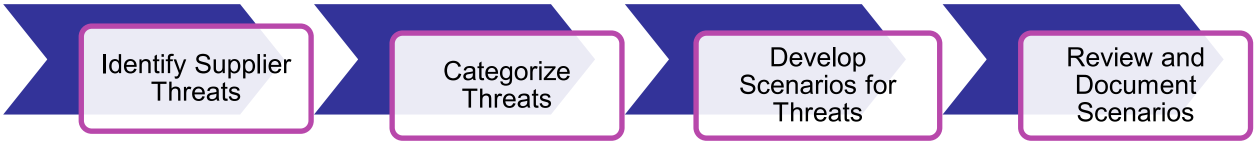
EXECUTIVE SUMMARY

Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of Information and Communications Technology (ICT) (including the Internet of Things) product and service supply chains. C-SCRM covers the entire life cycle of ICT, and encompasses hardware, software, and information assurance, along with traditional supply chain management and supply chain security considerations.

In October 2018, the Cybersecurity and Infrastructure Security Agency (CISA) launched the ICT Supply Chain Risk Management Task Force, a public-private partnership to provide advice and recommendations to CISA and its stakeholders on means for assessing and managing risks associated with the ICT supply chain. Working Group 2 (WG2), Threat Evaluation, was established for the purpose of the identification of processes and criteria for threat-based evaluation of ICT suppliers, products, and services.

WG2 focused on threat evaluation as opposed to the more comprehensive task of risk assessment which considers threats as well as an organization's tolerance for risk, the criticality of the specific asset or business/mission purpose, and the impact of exploitation of specific vulnerabilities that might be exploited by an external threat. The WG Co-chairs leveraged the National Institute of Standards and Technology (NIST) Risk Management Practices described in NIST SP 800-161 to help guide the analysis of the threats and threat sources identified in this work effort.

The general steps depicted in the figure below, and described in the following paragraphs, were used in the development and analysis of SCRM threats related to suppliers:


Identify Supplier Threats
Categorize Threats
Develop Scenarios for Threats
Review and Document Scenarios

The WG membership were asked to identify a representative sample of the top SCRM threats specifically focused on suppliers in accordance with our initial proposed scoping. Once the threats were identified, the WG proceeded to compile additional information fields identified in NIST SP 800-161 as elements to capture and refine with the WG members.

Each of the identified threats was then reviewed by the WG to develop a proposed set of common groupings and category assignments to organize the identified threats. Based on the presentation and analysis of the threats submitted by the WG members, the threats were aggregated into a smaller, more manageable set of common "threat grouping" to aid in the evaluation process. The objective of the aggregation was to reduce the threat data and identify common elements for further evaluation using a scenario development process.

This grouping and descriptive titles were shared with the WG membership for review and comment. While consensus was not unanimous, it was determined that for the purposes of the evaluation scope, the list of nine categories represented a reasonable model for aggregation for this interim work product. These threat groupings served to guide the development of scenarios intended to provide insights into the processes and criteria for conducting supplier threat assessment.

For each category, the WG assembled teams to develop a narrative/scenario in a report format that included background information on the threat itself, the importance of this threat, and potential impact on the supply chain. Multiple scenarios were developed for each category if deemed appropriate by the writing teams. A common format was developed to ensure that each threat scenario presented a comprehensive view of the specific threat aligned to the requirements of the information fields identified from NIST SP 800-161.

The process and resulting narratives not only serve as a baseline evaluation of specific SCRM threats, but further can be used as exemplary guidance on the application of the NIST Risk Management Framework. This process can be extended for evaluation of products and services, as well as replicated for other critical infrastructure providers. It also established a solid threat source evaluation that can be extended for specific products or services to drive the evaluation of SCRM risk.

Contents

1.0 Threat Evaluation Working Group Team Members 1
2.0 Background 3
2.1 Relationship between Threat, Vulnerability, and Risk 4
2.2 Relevant Definitions 4
3.0 Objective, Scope, and Methodology 5
3.1 Objective 5
3.2 Scope 5
3.3 Methodology 6
3.3.1 Focus on Supplier Threats — Data Gathering Process 7
3.3.2 Data Analysis 7
3.3.3 Threat Scenario Development 8
4.0 Findings 8
4.1 Supplier Threat List 8
4.1.1 Taxonomy of Threat List 8
4.1.2 Threat List 8
4.2 Threat Data Analysis 8
4.2.1 Categorization of Threats 8
4.2.2 Description of Threat Groups 9
4.2.2.1 Counterfeit Parts 9
4.2.2.2 Cybersecurity 9
4.2.2.3 Internal Security Operations and Controls 9
4.2.2.4 System Development Life Cycle (SDLC) Processes and Tools 9
4.2.2.5 Insider Threats 9
4.2.2.6 Economic Risks 10
4.2.2.7 Inherited Risk (Extended Supplier Chain) 10
4.2.2.8 Legal Risks 10
4.2.2.9 External End-to-End Supply Chain Risks (Natural Disasters, Geo-Political Issues) 10
4.2.3 Threat List Including Threat Groups 10
4.3 Threat Scenarios 10
4.3.1 Scenarios 10
5.0 Conclusions 10
Appendix A: Acronym List 12
Appendix B: Threat List 16
Appendix C: Threat Scenarios 33

Figures

Figure 1—Data Analysis Workflow 7

Tables

Table 1—Leadership and Administrative Support for Working Group 2 1
Table 2—Communications Sector Working Group Members 1
Table 3—Information Technology Sector Working Group Members 2
Table 4—U.S. Government Working Group Members 3
Table 5—Table Derived from NIST SP 800-161 6

1.0 THREAT EVALUATION WORKING GROUP TEAM MEMBERS

Leadership team for WG:

TABLE 1—LEADERSHIP AND ADMINISTRATIVE SUPPORT FOR WORKING GROUP 2

Co-Chair:	Drew Morin	T-Mobile
	Tommy Gardner	HP
	Angela Smith	GSA
Project Manager:	Julian Humble	DHS (SED)
Admin Support:	Josh Hyde	Contract Support (SED)
	Jaime Fleece	Contract Support (SED)

WG consists of the members listed below:

TABLE 2—COMMUNICATIONS SECTOR WORKING GROUP MEMBERS

Name	Company
Rich Mosely	AT&T
Jeff Huegel	AT&T
Jon Gannon	AT&T
Chris Boyer	AT&T
Kathryn Condello	CenturyLink
John Hayat	CenturyLink
Fernando Boza	CenturyLink
David Mazzocchi	CenturyLink
Dwight Steiner	CenturyLink
Melissa Brocato-Bryant	CenturyLink
Stephen Boggs	Cox
Rob Cantu	CTIA
Mike Kelley	E.W. Scripps Company
Eric Neel	Hubbard Broadcasting
Michael Iwanoff	Iconectiv
Larry Walke	National Association of Broadcasters
Kelly Williams	National Association of Broadcasters
Matt Tooley	NCTA
Jesse Ward	NTCA
Shamlan Siddiqi	NTT
Chad Kliewer	Pioneer
Mike Funk	Quincy Media
Diana Keplinger	Sprint
Greg Holzapfel	Sprint
Savannah Schaefer	TIA

Name	Company
Tanya Kumar	T-Mobile
Jessica Thompson	U.S. Telecom
Robert Mayer	U.S. Telecom
Michael Saperstein	U.S. Telecom
Frank Frontiera	Verizon
Chris Oatway	Verizon

TABLE 3—INFORMATION TECHNOLOGY SECTOR WORKING GROUP MEMBERS

Name	Company
Tom Topping	FireEye
Robert Wharton	HPE
C.J. Coppersmith	HPE
Ion Green	HPE
Mark Kelly	Dell
Trey Hodgkins	Hodgkins Consulting, LLC
John S. Miller	ITIC
Christopher "Travis" Miller	Interos
David Flowers	Interos
Randi Parker	CompTIA
Alvin Chan	HP
Melissa Bouilly	Dell
Tommy Ross	BSA
Jon Amis	Dell
Audrey Plonk	Intel
Ari Schwartz	Coalition for Cybersecurity Policy & Law
Geoff Kahn	Accenture
Marty Loy	Cisco
Jamie Brown	Tenable
Brad Minnis	Juniper - ITIC
Nick Boswell	CDW-G
Charlotte Lewis	CDW-G
Corey Cunningham	Rehancement Group
Peter McClelland	Threat Sketch
Tina Gregg	Microsoft
Jacob Crisp	Microsoft
Jason Boswell	Ericsson
Steve Lipner	SAFECode
Eric Nelson	Rehancement Group

TABLE 4—U.S. GOVERNMENT WORKING GROUP MEMBERS

Name	Company
Debra Jordan	FCC
Kurian Jacob	FCC
Dennis Martin	DHS
Ronald Clift	DHS
Beatrix Boyens	DHS
Michael Van de Woude	GSA
Jeremy P. McCrary	EOP/OMB
Jeffery Goldthorp	FCC
Rui Li	NRC
Patrick J. Kelly	OCC/Treasury
John Bowler	OCC/Treasury
Bradford "Brad" Bleier	FBI
Celia Paulsen (Prime)/Jon Boyens (Backup)	NIST
Michael Van de Woude	GSA
Gwen Hess	DHS
Scott Morrison	DOJ
Keith Nakasone (Prime)/Kelley Artz (Backup)	GSA
Stacy Bostjanick	DOD
Cherylene G. Caddy	NSA
Anita J. Patankar-Stoll	NSC
Evan Broderick	NTIA
Megan Doscher	NTIA
Scott Friedman	DHS
Evelyn Remaley	NTIA
Ganiu "Tosin" Adegun	NASA
Michael "Mike" Bridges	NASA
Kanitra Tyler	NASA

2.0 BACKGROUND

In October 2018, CISA launched the Information and Communications Technology Supply Chain Risk Management (ICT SCRM) Task Force, a public-private partnership to provide advice and recommendations to the CISA and its stakeholders on means for assessing and managing risks associated with the ICT supply chain.

The ICT SCRM Task Force provides a mechanism for representatives of industry and government, designed to share information, explore challenges, and develop recommendations to manage ICT supply chain risks. The Task Force is led by representatives of DHS and the Communications and Information Technology sectors. Task Force membership and participation represents the public-private, cross-sector nature of the Task Force, with members drawn from both sectors and from across the government.

The Task Force summarized the results of its first year of work in the ICT SCRM Task Force Interim Report, which was released in September 2019 and can be found HERE (https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf). This Interim Report includes a description of the Task Force's progress and an initial set of recommendations, derived from the individual reports of the Task Force's four WGs. The Interim Report and the reports of the subordinate WGs memorialize the work of these collaborative bodies, including consensus recommendations provided through the Critical Infrastructure Partnerships Advisory Council process to the federal agency participants. The activity of federal employees on the task force, including participation in discussions and votes, is intended to inform the Task Force's work through the individual experience of the participating members as subject matter experts and does not necessarily represent the official position of, or adoption of any recommendation by, the U.S. government or any represented Federal department or agency.

The Task Force evaluated multiple potential work streams and reached consensus on the establishment of four Task Force WGs and an Inventory WG. WG, Threat Evaluation, was established for the purpose of the **identification of processes and criteria for threat-based evaluation of ICT suppliers, products, and services**. This proposed work stream is intended to provide ICT buyers and users with assistance and guidance for evaluating supply chain threats. Bringing uniformity and consistency to this process will benefit government and industry alike.

2.1 Relationship between Threat, Vulnerability, and Risk

A thing (threat source) interacts with a weakness (vulnerability) which results in something bad happening (threat event). The way the source interacted with the weakness is a *threat vector*. If the threat source was a human and the event intentional, it is an *attack*.

A vulnerability is a shortcoming or hole in the *security* of an asset. Risk represents the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities.

2.2 Relevant Definitions

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (FIPS 200)

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. (FIPS 200)

Threat event: An event or situation that has the potential for causing undesirable consequences or impact. (NIST SP 800-30)

Threat source / agent: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. (FIPS 200)

Attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality. (NIST SP 800-82 & CNSSI 4009)

3.0 OBJECTIVE, SCOPE, AND METHODOLOGY

Working Group 2 is focused on Threat Evaluation as opposed to risk assessment since risk is specifically associated with an asset (product, service, supplier in the case of the charter for this ICT C-SCRM Task Force).

The WG Co-chairs leveraged the NIST Risk Management Practices described in NIST SP 800-161 to help guide the analysis of the threats and threat sources identified in this work effort.

3.1 Objective

ICT Task Force WG, Threat Evaluation, was chartered with the identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services. The objectives of this Threat Evaluation were defined as:

- Produce a set of processes and criteria for conducting supplier, product, and service threat assessments.
- The processes and criteria will initially be focused only on global ICT supplier selection, pedigree, and provenance. It will also address product assurance (hardware, software, firmware, etc.), data security, and supply chain risks.
- Finally, the process and criteria will establish a framework for a threat-based assessment of cyber supply chain risks that can be extended in future work products to address other critical infrastructure sectors.

3.2 Scope

The ICT C-SCRM Task Force agreed early on to leverage the NIST definition for C-SCRM and to scope according to the Federal Acquisition Supply Chain Security Act.

NIST definition: Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of ICT product and service supply chains. C-SCRM covers the entire life cycle of ICT:

- Encompasses hardware, software, and information assurance, along with traditional supply chain management and supply chain security practices.[1]

Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Subchap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018)

Covered articles means:

- Information technology, including cloud computing services of all types (41 USC 4713(k)(2)(A));
- Telecommunications equipment or telecommunications service (41 USC 4713(k)(2)(B));
- The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (41 USC 4713(k)(2)(C));
- All Internet of Things/Operational Technology (IoT/OT) – (hardware, systems, devices, software, or services that include embedded or incidental information technology). (41 USC 4713(k)(2)(D)).

[1] See, NIST definition of C-SCRM, available at: https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management. For purposes of the ICT SCRM Task Force, the term "ICT" includes operational technology and "Internet of Things" devices and services.

3.3 Methodology

The WG initially conducted a survey of threat information from the diverse WG membership. The only constraint on the identification of threats was to focus on supplier threats in accordance with our initial proposed scoping. The methods developed and applied in our initial supplier threat evaluation process will be repeatable in future iterations as the WG proceeds to expand our scope to include products and services.

Once the threats were identified, the WG proceeded to complete the additional information captured in the fields highlighted in green from the NIST SP 800-161 spreadsheet in table 5 below as elements to capture and refine with the WG members. Information was captured in the current WG2 Supply Chain Threats by adding a few additional columns. This information was then used to inform the threat analysis process for supplier evaluation.

TABLE 5—TABLE DERIVED FROM NIST SP 800-161

Threat Scenario	**Threat Source**	*Threat "actor" or category of threats*
	Vulnerability	*Threat list Working group has generated*
	Threat Event Description	*Description of the method(s) of exploiting the vulnerability*
	Outcome	*Description of potential impacts to Supply Chain or consequences of exploiting the vulnerability*
Organizational units / processes affected		*This should reflect how/where in the supply chain the impact occurs*
Risk	**Impact**	
	Likelihood	
	Risk Score (Impact x Likelihood)	
	Acceptable Level of Risk	
Mitigation	**Potential Mitigating Strategies / SCRM Controls**	*Identify supplier evaluation criteria that would reduce or mitigate the impact of the threat*
	Estimated Cost of Mitigating Strategies	
	Change in Likelihood	
	Change in Impact	
	Selected Strategies	
	Estimated Residual Risk	

The remaining fields not completed by this WG represent the asset specific data that is captured to assess risk; something that will vary considerably depending on the specific supplier/product/service. This will result in a work product that will be consistent with NIST guidance concerning threat and flexible to be used by industry and public sector for a variety of purposes.

The WG executed using an iterative process with interim deliverables shareable between the other Task Force WGs to inform their efforts. For example, the threats identified by WG2 were shared with and used to inform the Information Sharing WG on threat focus areas for information gathering and sharing. Similarly, the threats identified were leveraged to aid in assessing the inventory of standards and best practices that may be applicable to the evolving C-SCRM threat environment.

3.3.1 FOCUS ON SUPPLIER THREATS — DATA GATHERING PROCESS

This section describes the process used to generate the threats to SCRM suppliers and the sharing of those threats as inputs to the evaluation to follow. It should be noted that these threats are not considered comprehensive, but rather are representative, such that the evaluation WG could proceed through the exercise of threat evaluation put forward by the NIST Risk Management Framework.

The WG members considered C-SCRM Threats from a variety of sources including Industry Subject Matter Experts (SME), Department of Defense (DoD), Intelligence Community (IC), Department of Homeland Security (DHS), and others to inform the development of risk-based criteria. The first data call conducted was a request from WG membership to provide supply chain threats that they recognize from their own experience or from their organization's perspective.[2] The requested format of the data call was a bulleted list describing each threat. Our purpose was to initially cast a wide net to capture a broad sample of threat inputs for analysis.

Each threat submitted was presented by the WG member that sourced the information to the broader membership. The discussion enabled the WG to process additional details on each threat with the stated purpose of gaining a shared understanding of the specific threats identified. This process was repeated, and notes were captured for each of the identified threats. This set of information was compiled into a single data repository that was used in the Data Analysis phase of the process described below.

3.3.2 DATA ANALYSIS

The WG proceeded to review and categorize the collected data to develop useful insights into the current state of supplier threats in both public and private sectors. The threats identified by the WG members were then consolidated and grouped to provide a manageable and shareable set of threat groupings for further the development of specific scenarios. These threat groupings served to guide the development of scenarios intended to provide insights into the processes and criteria for conducting supplier threat assessment.

As part of our analysis, the WG membership considered existing business due diligence indicators, such as those listed in General Services Administration's (GSA) Request for Information (RFI), Office of the Comptroller of the Currency (OCC) Third Party Risk Management guidance, and industry best practices identified as part of the inventory work product. Figure 1 below depicts the flow used by the WG to conduct the data analysis.

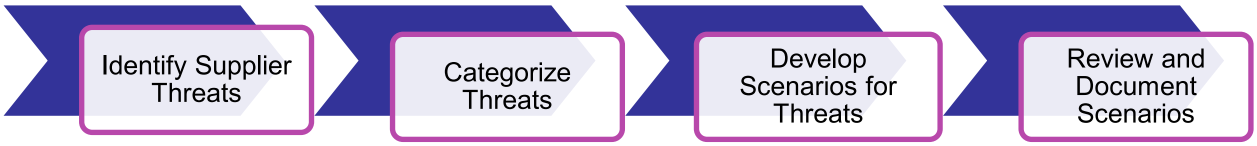

Identify Supplier Threats
Categorize Threats
Develop Scenarios for Threats
Review and Document Scenarios

FIGURE 1—DATA ANALYSIS WORKFLOW

[2] The working group data call requested each member to provide between five and ten supplier threats. The result was an initial set of over 250 specific threats.

3.3.3 THREAT SCENARIO DEVELOPMENT

Once the WG has established supply chain threat categories, the WG assembled teams for each category. Each team then provided a narrative/scenario developed in a report format that includes **background information on the threat itself, the importance of this threat, and potential impact on the supply chain**. Multiple scenarios were developed for each category if deemed necessary by the writing teams. Each scenario also includes details surrounding the:

- **What** (Description of the threat category. Text could include example threats associated with the category),
- **Who** (Who is likely to be the source of the threat [e.g., nation state, organized crime] and who the likely target of the threat is),
- **When – If applicable** (Is the timing of the attack? Is it Denial of Service or zero day? Is it persistent or a one-time event? Etc.),
- **Why** (Objective of threat actors, intellectual property theft, network disruption…), and
- **Where** (Where in the Supply chain the specific threat activity is occurring).

A common format was developed to ensure that each threat scenario presented a comprehensive view of the specific threat aligned to the requirements of the information fields identified from NIST SP 800-161 as described in Section 2.0 above.

4.0 FINDINGS

4.1 Supplier Threat List

This section describes the supplier threat information gathered and the specific information for each threat that was presented for evaluation by the WG membership.

4.1.1 TAXONOMY OF THREAT LIST

The initial data call from the WG members was for the identification of supplier threats. The scope of the threats was intentionally left broad to not restrict the identification process. A limited set of information was provided for each threat by the WG member that sourced the information.

- Threat description: Short text description of the specific supplier threat
- Threat category (provided by source): Identification of the category that the WG member assigned to the identified threat
- Threat source: Identification of the source or sources that might exploit the vulnerability identified by the threat

4.1.2 THREAT LIST

The threats identified were presented to the entire WG to enable a common understanding of the information provided concerning each specific threat. The list was then consolidated based on common threat categories and reviewed with the WG membership to gain consensus.

4.2 Threat Data Analysis

4.2.1 CATEGORIZATION OF THREATS

Once the threat list was populated, the co-chairs reviewed the categories assigned to each of the threats to aggregate specific threats into a smaller, more manageable set of common threat groups. The objective of the aggregation was to reduce the threat data and identify common elements for further evaluation using a scenario development process.

In order to aggregate the data, common threat categories were first identified. The next step of the analysis was to group the threats that shared common and related threat categories. Each of the identified threats was then reviewed by the WG to ensure that the common groupings and category assignments accurately reflected the threat. A few of the threats initially identified were dropped from the list as they did not actually represent threats (for example, some were impacts or use case specific risks).

Once the threat category review was completed, the co-chairs proposed a set of threat groups to represent the set of common categories of threats identified. This grouping and descriptive titles were shared with the WG membership for review and comment. While consensus was not unanimous, it was determined that for the purposes of the evaluation scope, the list of nine categories represented a reasonable model for aggregation.

4.2.2 DESCRIPTION OF THREAT GROUPS

The evaluation of the threats submitted by the broad spectrum of WG members was consolidated into logical threat groups to aid in the evaluation process. The description of each of these threat groupings is provided in the following sections.

4.2.2.1 Counterfeit Parts

Insertion of counterfeits in the supply chain can have severe consequences in systems and services provided to downstream customers. These threats are associated with the replacement or substitution of trusted or qualified supplier components, products, or services with those from potentially untrusted sources.

4.2.2.2 Cybersecurity

This threat category represents those that result from the set of vulnerabilities associated with external attacks on suppliers' operations and capabilities. These threats are the result of an external actor exploiting a vulnerability or planting malware attack such as zero day or malware with an objective of compromising the confidentiality, integrity, or availability of the supplier information, products, or services.

4.2.2.3 Internal Security Operations and Controls

This category of threats is closely related to cybersecurity identified above. The primary differentiator is that these threats are a result of challenges in internal supplier processes that enable the exploitation of weaknesses in basic cyber hygiene (e.g., software patching), user awareness (e.g., spear phishing), mishandling of sensitive information, or internal cybersecurity process failures from the lack of a cybersecurity program based on best practices such as the NIST Cybersecurity Framework.

4.2.2.4 System Development Life Cycle (SDLC) Processes and Tools

This threat category represents those threats that impact the suppliers' ability to develop products or services that protect the confidentiality, integrity, and availability of products and services developed by the supplier.

An example of this group of threats include failures in the development process to detect introduction of malware or unvetted code into software products through use of vulnerable open source libraries.

4.2.2.5 Insider Threats

This category of threats focuses on the vulnerability of the supplier to attack from trusted staff and partners that are embedded internal to the supplier operations. Most of the threats identified in this grouping are associated with intentional tampering or interference.

4.2.2.6 Economic Risks

Economic risks stem from threats to the financial viability of suppliers and the potential impact to the supply chain resulting from the failure of a key supplier as a result. Other threats to the supply chain that result in economic risks include, but are not limited to, vulnerabilities to cost volatility, reliance on single source suppliers, cost to swap out suspect vendors, and resource constraints as a result of company size.

4.2.2.7 Inherited Risk (Extended Supplier Chain)

This category of threats is a result of current supply chains that extend broadly across industries and geographies. These threats typically are associated with the challenge of extending controls and best practices through the entire supply chain due to its global nature. It also includes the vulnerabilities that can result from integration of components, products, or services from lower tier supplier where a prior determination of acceptable risk may not flow all the way through the development process to the end user supplier.

4.2.2.8 Legal Risks

This category of threats emanates from supplier vulnerabilities specific to legal jurisdiction. Some examples include weak anti-corruption laws, lack of regulatory oversight, weak intellectual property considerations. This also includes the threats that result from country specific laws, policies, and practices intended to undermine competition and free market protections such as the requirement to transfer technology and intellectual property to domestic providers in a foreign country.

4.2.2.9 External End-to-End Supply Chain Risks (Natural Disasters, Geo-Political Issues)

This category of threats is associated with broad based environmental, geopolitical, regulatory compliance, workforce and other vulnerabilities to the confidentiality, integrity or availability of supplier information, products or services.

4.2.3 THREAT LIST INCLUDING THREAT GROUPS

The threat list compiled based on the data analysis presented is included as Appendix B to this document.

4.3 Threat Scenarios

4.3.1 SCENARIOS

The Threat Evaluation WG – Supplier Threat Scenarios developed for the ICT SCRM Task Force is included as Appendix C to this document.

5.0 CONCLUSIONS

The WG kicked off this evaluation with a blank sheet and focused on leveraging the diversity of our membership to provide a broad base of threats for analysis and evaluation.

This interim report and threat evaluation is limited to supplier threats only. The WG membership recognize that some of these threats are also applicable to products and services.

The methods developed and applied in our initial supplier threat evaluation process will be repeatable in future iterations as the WG proceeds to expand our scope to include products and services.

The WG struggled with the specific threat groupings used, including proposal for further aggregation of the threat groupings into common sets to provide further clarification of the definition of each threat grouping. There were also some concerns that the threats identified may have also included risks. Due to time constraints, the co-chairs captured this information but decided to defer this to potential follow on work on products and services. This assumes that the task force supports the WG guidance to continue this work effort in the next iteration of WG outputs.

The WG recommends that the task force continue the charter for this effort with a focus on addressing products and services, review of categorization of threats, and possibly to provide risk assessments of some specific threats, prioritized by membership, as examples of how to leverage this threat assessment as an information feed into a company specific risk management program.

APPENDIX A: ACRONYM LIST

BGP	Border Gateway Protocol
BIA	Business Impact Analysis
CAD	Computer-Assisted Design
CCTV	Close-Circuit Televisions
CERT	Computer Emergency Readiness Team
CFIUS	Committee on Foreign Investment in the United States
CIS	Center for Internet Security
CSRIC	Communication, Security, Reliability, and Interoperability Council
C-SCRM	Cyber Supply Chain Risk Management
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DOJ	Department of Justice
EAS	Emergency Alert System
FAR	Federal Acquisition Regulation
FCC	Federal Communications Commission

FIPS	Federal Information Processing Standards
GSA	General Services Administration
HPE	Hewlett-Packard Enterprises
ICT	Information and Communications Technology
ID	Identification
IP	Internet Protocol
IP*	Intellectual Property
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITAM	Information Technology Asset Management
ITIC	Information Technology Industry Council
ITP	Insider Threat Program
MAC	Media Access Control
MANRS	Mutually Agreed Norms for Routing Security
NASA	National Aeronautics and Space Administration
NDA	Non-Disclosure Agreement
NIST-SP	National Institute of Standards and Technology (NIST) Special Publication

NTIA	National Telecommunications and Information Administration
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OS	Operating System
OT	Operational Technology
PAM	Privileged Access Management
PC	Personal Computer
PCB	Printed Circuit Board
PWB	Printed Wiring Board
SAM	Software Asset Management
SC	Semiconductor
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SED	Stakeholder Engagement Division
SMB	Small and Medium-sized Business
SNMP	Simple Network Management Protocol
SPVM	Sourcing, Procurement and Vendor Management
SQL	Standardized Query Language

SSH	Secure Shell
TAA	Trade Agreements Act
TIA	Telecommunications Industry Association
U.S.	United States
USB	Universal Serial Bus
VPN	Virtual Private Network
WG	Working Group

APPENDIX B: THREAT LIST

Note: The WG membership were asked to identify a representative sample of the top SCRM threats specifically focused on suppliers in accordance with our initial proposed scoping. Based on presentation and analysis of the threats submitted by the WG members, the items were aggregated into a smaller, more manageable set of common threat groupings to aid in the evaluation process. The objective of the aggregation was to identify common elements for further evaluation using a scenario development process. The threats identified represent the output produced by this methodology, and do not represent an official or consensus documentation of supply chain threats. The threat list is intended to document the WG's work and provide input for future policy discussions.

Threats	Threat Categories or Event	Threat Source or Actor
Counterfeit Parts		
Counterfeit product or component with malicious intent to cause unwanted function	Adversarial: Craft or create attack tools	Nation state; organization; individual (Outsider/Insider)
Component elements included in product, software, or service		
Virtualization and encapsulation hiding access		
Sales of modified or counterfeit products to legitimate distributors		
A malicious supplier employee inserts hostile content at the product or component manufacturing or distribution stage so as to affect supplier products or components delivered to a subset (potentially a targeted subset) of downstream customers. (Tampering or counterfeiting)		
Insert tampered critical components into organizational systems	Adversarial: Deliver, insert, or install malicious capabilities	

Insert counterfeit or tampered hardware into the supply chain		Nation state; Organization; Individual (Outsider/Insider)
Counterfeit product or component without malicious intent to cause unwanted function	Accidental: User; privileged user	Individual (Insider)
Create counterfeit or spoof website	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Craft counterfeit certificates	Adversarial: Craft or create attack tools	Nation state; Organization
Embedded HW/SW threats from non-OEM source(s)	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Cybersecurity		
Data breaches and unauthorized access to sensitive data (at rest and in transit)	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider/Insider)
Loss of critical information from vendor		
Obtain unauthorized access		
Data - Impacts to confidentiality, Integrity or availability		
Malware, unauthorized access, theft		
Cause unauthorized disclosure or unavailability by spilling sensitive information		
Spill sensitive information	Accidental: User; privileged user	Individual (Insider)

Login Attacks (Brute force, Dictionary attacks, Password spraying)	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider)
Credential Compromise		
Supplier solution architecture allows for manipulation and extraction of data and services (Not due to a system vulnerability)	Accidental: User, privileged user	Nation state; Organization; Individual (Outsider/Insider)
Phishing, spear phishing, or whaling	Adversarial: Craft or create attack tools	Nation state; Organization;
Malware, unauthorized access, theft		
Deliver known malware to internal organizational information systems (e.g., virus via email)	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider)
Compromise of integrity of product through intrusion	Adversarial: Exploit and compromise	Nation state; Organization; Individual (Outsider)
External cyber attacker threats		
Embedded malware or virus attacks in delivered products	Adversarial: Craft or Create Attack Tools	Nation state; Organization; Individual (Outsider/Insider)
Inappropriate modification of device, software, or service through network update		
Embedded HW/SW threats (from manufacturing)		

A malicious supplier employee inserts hostile content at the product or component manufacturing or distribution stage so as to affect supplier products or components delivered to a subset (potentially a targeted subset) of downstream customers. (Tampering or counterfeiting)		
Embedded Malware. Virus Attacks in hosted services websites	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Malware disguised as driver updates or system patches on compromise vendor web site		
Intrusion or compromise of customer through service		
Inappropriate modification of device, software, service through network update		
Product vulnerabilities (intended) in hardware and software	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Product vulnerabilities (unintended) in hardware and software	Accidental: User, privileged user	Individual (Insider)
Resource depletion		
Pervasive disk error		
Advanced Persistent Threats	Adversarial: Maintain a presence	Nation state; Organization
DNS attack	Adversarial: Conduct an attack	Nation state; Organization
DoS/DDoS	Adversarial: Conduct an attack	

Threat actor impacts app store availability impacting end user ability to do job		Nation state; Organization; Individual (Outsider)
Threat actor hacks cloud environment or telco making service unavailable		
Threat actor breaks ability of information provider to deliver information		
Man in the middle attack	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider)
Obtain information by externally located interception of wireless network traffic		
Incorrect BGP routing at a level above your network		
Replay attack	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider)
Spoofing	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider)
URL injection	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider)
Intentional specific software security threats or vulnerabilities exploitation (long list of specific types not included for brevity)	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Threat actor compromises or hacks it software		
Unintentional specific software security threats or vulnerabilities exploitation (long list of specific types not included for brevity)	Accidental: User, privileged user	Individual (Insider)

System misconfiguration	Accidental: User, privileged user	Nation state; Organization; Individual (Outsider/Insider)
Zero-Day exploits	Adversarial: Craft or create attack tools	Nation state; Organization
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware	Adversarial: Conduct an attack (i.e., direct or coordinate attack tools or activities)	Nation state; Organization
Perform malware- directed internal reconnaissance	Adversarial: Perform reconnaissance and gather information	Nation state; Organization
Craft attacks specifically based on deployed information technology environment	Adversarial: Craft or create attack tools	Nation state; Organization
Deliver modified malware to internal organizational information systems	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Deliver targeted malware for control of internal systems and exfiltration of data	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Deliver malware by providing removable media	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization
Exploit split tunneling	Adversarial: Exploit and compromise	Nation state; Organization
Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo	Adversarial: Exploit and Compromise	Nation state; Organization; Individual (Outsider/Insider)

Violate isolation in multi-tenant environment	Adversarial: Exploit and Compromise	Nation state; Organization
Compromise information systems or devices used externally and reintroduced into the enterprise	Adversarial: Exploit and Compromise	Nation state; Organization
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome	Adversarial: Maintain a presence or set of capabilities	Nation state; Organization
Coordinate cyber-attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors	Adversarial: Maintain a presence or set of capabilities	Nation state; Organization
Purchasing of equipment with known critical security vulnerabilities (example: nearly all Android based cellphones) and little expectation of patching by vendor	Accidental: User, privileged user	Individual: Insider
Compromise of integrity of virtualization	Adversarial: Exploit and compromise	Nation state; Organization; Individual (Outsider/Insider)
Access through service contract	Adversarial: Maintain a presence or set of capabilities	Nation state; Organization
Quantum computing threat to commercial cryptography	Adversarial: Exploit and compromise	Nation state
Cryptojacking	Adversarial: Exploit and compromise	Nation state; Organization
Ransomware	Adversarial: exploit and compromise	Nation state; Organization
Conduct physical attacks on infrastructures supporting organizational facilities	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider/Insider)
Physical compromise of specific device		

Physical access through presence of device	Adversarial: Exploit and compromise	Nation state; Organization; Individual (Outsider/Insider)
Physical network control or access		
Physical control of infrastructure		
Threat actor activity overwhelms organizations ability to deal with attacks, IT supply chain-services unable to surge to meet need	Adversarial: Conduct an attack	Nation state; Organization
Internal Security Operations and Controls		
Lack of knowledge (suppliers or subcontractors, especially SMBs, not knowing what their vulnerabilities are)	Accidental: Deliver, insert, install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Product vulnerabilities (advertent or inadvertent) in hardware and software	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Vulnerability Exploitation		
Supplier Has Weak Controls To Detect Or Prevent Social Engineering	Accidental: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider)
Data And Media Disposal Is Not Secure-Allowing Disclosure Of Sensitive Data	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider)
Obtain information by opportunistically stealing or scavenging information systems/components.		
Exploit insecure or incomplete data deletion in multi-tenant environment.	Adversarial: Exploit and Compromise	Nation state; Organization; Individual (Outsider)
Data breaches post disconnect		

Poor Employee/Contractor/Vendor Access Controls	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider/Insider)
Supplier System Does Not Have Controls To Validate And Authorize Escalation Of Privileges		
Staff using vulnerable unpatched personal computer systems from home to contact agency resources	Accidental: Individual	Individual (Outsider/Insider)
Large enterprise (~$10 billion / year) that supplies key components for mission projects continues to experience cyberattack and illicit technology transfer events	Adversarial: Exploit and Compromise	Nation state; Organization; Individual (Outsider)
ICT Devices with default passwords	Accidental: Deliver, insert, or install malicious capabilities	Organization
(Removal of) Hardset accounts in devices and software		
Devices that do not auto-update firmware	Accidental: Deliver, insert, or install malicious capabilities	Organization
Mishandling of critical or sensitive information by authorized users	Accidental: Individual	Individual (Insider)
Incorrect privilege settings	Accidental: Individual	Individual (Insider)
The nuclear power section has a maturing cyber program or defense architecture and regulatory requirements, but sophisticated offensive groups with nation states capabilities are threats	Accidental: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider)
Compromise of SDLC Processes and Tools		
Malware coded, inserted, or deployed into critical ICT throughout the design,		

development, integration, deployment or maintenance phase of components	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Manipulation of development tools		
Manipulation of a development environment		
Manipulation of source code repositories (public or private)		
Manipulation of software update/distribution mechanisms		
Compromise design, manufacture, or distribution of information system components (including hardware, software, and firmware)	Adversarial Supply Chain Threat: Exploit and compromise	Nation state; Organization; Individual (Outsider/Insider)
Compromised/infected system images (multiple cases of removable media infected at the factory)	Adversarial: Exploit and Compromise	Nation state; Organization; Individual (Outsider/Insider)
Replacement of legitimate software with modified versions	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Insert untargeted malware into downloadable software or into commercial information technology products.		
Insert targeted malware into organizational information systems and information system components.	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Insert specialized malware into organizational information systems based on system configurations.	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Introduction of vulnerabilities into software products from open source	Accidental: Individual	Individual (Outsider/Insider)

Software integrity and does the product include open source code		
Foreign developed computer code or source code	Accidental: Individual or privileged user	Nation state; Organization; Individual (Outsider/Insider)
Foreign companies controlled or influenced by a foreign adversary	Adversarial: Maintain a presence or set of capabilities	Nation state
Insider Threat		
Lone wolf (disgruntled employee)	Adversarial: Conduct an attack	Individual: Insider
Insider threats	Adversarial: Deliver, insert, or install malicious capabilities.	Nation state; Organization; Individual (Outsider/Insider)
Threat actor recruits onsite IT services personnel with gambling debts to spy		
IT services supply chain sends spy onsite		
Insert subverted individuals into organizations		
Insert subverted individuals into privileged positions in organizations		
Internal: Personnel Threat		
Conduct internally based session hijacking	Adversarial: Conduct an attack	Individual: Privileged Insider
Tampering while on hand	Adversarial: Conduct an attack	Individual (Outsider/Insider)
Tampering while being deployed or installed	Adversarial: Conduct an attack	Individual (Outsider/Insider)

Tampering while being maintained	Adversarial: Conduct an attack	Individual (Outsider/Insider)
Tampering while being repaired	Adversarial: Conduct an attack	Individual (Outsider/Insider)
Economic		
Viability of financially weak suppliers	Economic: Financial stability	Nation state; Organization
Financial Stability	Economic: Financial stability	Nation state; Organization
Economic risk (i.e. a supplier or sub-contractor of a supplier will be economically devastated by a breach).	Economic: Financial stability	Nation state; Organization
Limited visibility into business and sustainability practices of suppliers beyond the first tier	Economic: Financial stability	Organization
Cost Volatility	Economic: Financial stability	Organization
No vendor support when a company transfers ownership or closes	Economic: Financial stability	Organization
Operational disruptions due to source being acquired by a far larger company with questionable security		
Very small, privately-held company “one-man show” with inadequate quality management with history of delivery delays and security concerns contracted to product components on the critical path of multiple mission projects	Economic: Financial stability	Organization
Young entrepreneurial business identified as a potential subcontractor for key mission components but has no discoverable facility for production, integration, test, nor quality management		

SMB often lack the ability to heavily influence vendors to correct issues	Economic: Production problems	Organization
Little control over what applications or devices customers use or connect via our services	Economic: Production problems	Organization; Individual (Outside)
If a vendor is compromised, some providers that use the same equipment or software across their entire system do not have the resources to continue operations or switch to another vendor	Economic: Production problems	Nation state; Organization; Individual (Outsider/Insider)
Threat Actor Determines How To Manipulate Decision By Delivering Too Much, Too Little, or Type of Information. It's Not Inaccurate, Yet It Somehow Changes Decisions	Economic: Production problems	Nation state; Organization; Individual (Outsider/Insider)
Industry Discovers Vulnerability In IT Product X Resulting In Freeze In Using That Product Until Fixed.	Economic: Production problems	Nation state; Organization; Individual (Outsider/Insider)
Small and many medium sized businesses do not have the resources or expertise to evaluate the security of all devices and software that are purchased by the company	Economic: Production problems	Organization
Most small and medium sized providers do not proactively monitor customer-based equipment for anomalous behaviors, and as such are unable to diagnose a security issue unless notified by other means	Economic: Production problems	Organization
Inherited Risk (Extended Supplier Chain)		
Inherited risk (extended supplier chain)	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Inherited risk generally		

Mid supply chain insertion of counterfeit parts		
Depth of the supply chain and who is supplying the supplier		
Domestic Companies		
Lack of enforced traceability		
Supplier incorporates hostile content in product or component		
Threat of upstream intrusions in supply chain and lack of traceability from component to finished product		
Supplier has malicious intent and incorporates hostile content in product or component. This scenario applies to hardware or software providers (including both proprietary and open source software)		
Trustworthy supplier inadvertently creates a product or component that is vulnerable to attack and delivers it to downstream customers. This scenario applies to hardware or software providers (including both proprietary and open source software).		
Tampering while in transit	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider/Insider)
Shipment interdiction		
Vendor noncompliance	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Lack of Certification of component safety or quality at each appropriate level of the value chain of a product		

Integrity of integrated third-party components		
Lack of oversight or security standards for imported devices		
NRC does not have direct authority over third party suppliers.		
Lack of required disclosure of component manufacturer origin	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Lack of disclosure of origin		
Create and operate false front organizations to inject malicious components into the supply chain	Adversarial: Craft or create attack tools	Nation state; Organization
IT information provider delivers intentionally bad or misleading data (e.g. DNS/BGP)	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider/Insider)
A malicious supplier employee inserts hostile content at the product or component design or software coding stage so as to affect a large number of supplier products or components. (Tampering)	Adversarial: Achieve results	Individual (Insider)
An upstream supplier to the trustworthy supplier serves as a vehicle (witting or unwitting) for introduction of hostile content into a hardware or software component that the trustworthy supplier in turn integrates into its product or component and delivers to downstream customers. (Tampering or counterfeiting)	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider/Insider)
An external threat actor penetrates the trustworthy supplier’s design or manufacturing systems and inserts hostile content into a product or component that the trustworthy supplier	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider)

delivers to downstream customers (Tampering)		
Legal risks		
Legal: IP or Licensing violation	Legal: IP or Licensing violation	Nation state; Organization; Individual (Outsider/Insider)
Suppliers operating in countries with weak Intellectual Property (IP) protection laws		
Liability for purchaser	Legal: Lawsuits	Nation state; Organization
Supplier fear liability impact could devastate participants in supply chain, particularly SMBs	Legal: Lawsuits	Nation state; Organization; Individual (Outsider/Insider)
Privacy regulations	External: Government compliance and political uncertainty	Nation state; Organization
Legislation and compliance	External: Government compliance and political uncertainty	Nation state; Organization
Known to engage in financial crimes (e.g. fraud, bribery, money laundering, etc.)	External: Legal noncompliance or ethical practices	Organization
Known to have violated U.S. sanctions		
External, End-to-End Supply Chain Risks		
Natural disaster causing supply chain disruptions	External: Natural disasters	Environmental: Natural
Natural disaster		
Natural disruptions		

Geo-Political uncertainty	External: Government compliance and political uncertainty	Nation state; Organization
Man Made Disruptions: sabotage, terrorism, crime, war	External: Government compliance and political uncertainty	Nation state; Organization
Labor issues	External: Government compliance and political uncertainty	Nation state; Organization
Supply chain disruptions and price spikes due to protectionism in global trade	External: Government compliance and political uncertainty	Nation state
Lack of legislative governance enforcing traceability within the manufacturing and assembly process.	External: Government compliance and political uncertainty	Nation state; Organization
Nation state control over foreign suppliers	External: Government compliance and political uncertainty	Nation state
Diminishing contribution of U.S. companies in technology standards bodies and open source software	Adversarial: Maintain a presence or set of capabilities.	Nation state

APPENDIX C: THREAT SCENARIOS

Appendix C: Threat Scenarios 33
6.0 Threat Category: Counterfeit Parts 39
6.1 Scenario: Service Contracts 39
6.1.1 Background 39
6.1.2 Threat Source 39
6.1.3 Vulnerability 39
6.1.4 Threat Event Description 39
6.1.5 Outcome 39
6.1.6 Organizational Units / Processes Affected 39
6.1.7 Potential Mitigating Strategies / SCRM Controls 40
6.2 Scenario: Asset Management, specifically Software Asset Management (SAM). 40
6.2.1 Background 40
6.2.2 Threat Source 40
6.2.3 Vulnerability 40
6.2.4 Threat Event Description 40
6.2.5 Outcome 40
6.2.6 Organizational Units / Processes Affected 41
6.2.7 Potential Mitigating Strategies / SCRM Controls 41
6.3 Scenario: Yokogawa Electric Corporation Counterfeit Equipment 41
6.3.1 Background 41
6.3.2 Threat Source 41
6.3.3 Vulnerability 42
6.3.4 Threat Event Description 42
6.3.5 Outcome 42
6.3.6 Organizational Units / Processes Affected 42
6.3.7 Potential Mitigating Strategies / SCRM Controls 42
7.0 Threat Category: Cybersecurity 42
7.1 Scenario: Incorrect Border Gateway Protocol (BGP) Routing 42
7.1.1 Background 42
7.1.2 Threat Source 42
7.1.3 Vulnerability 42
7.1.4 Threat Event Description 42
7.1.5 Outcome 43
7.1.6 Organizational Units / Processes Affected 43
7.1.7 Potential Mitigating Strategies / SCRM Controls 43
7.2 Scenario: Ransomware Attack 43
7.2.1 Background 43
7.2.2 Threat Source 43
7.2.3 Vulnerability 43
7.2.4 Threat Event Description 43
7.2.5 Outcome 44
7.2.6 Organizational Units / Processes Affected 44
7.2.7 Potential Mitigating Strategies / SCRM Controls 44
7.3 Scenario: Removable Media Attack 45
7.3.1 Background 45

7.3.2 Threat Source..45
7.3.3 Vulnerability..45
7.3.4 Threat Event Description..45
7.3.5 Outcome..46
7.3.6 Organizational Units / Processes Affected..46
7.3.7 Potential Mitigating Strategies / SCRM Controls..46
7.4 Scenario: Resource Depletion – Unintentional/Accidental Shutdown..46
7.4.1 Background..46
7.4.2 Threat Source..47
7.4.3 Vulnerability..47
7.4.4 Threat Event Description..47
7.4.5 Outcome..47
7.4.6 Organizational Units / Processes Affected..47
7.4.7 Potential Mitigating Strategies / SCRM Controls..47
8.0 Threat Category: Internal Security Operations and Controls..48
8.1 Scenario: Poor Access Control Policy..48
8.1.1 Background..48
8.1.2 Threat Source..48
8.1.3 Vulnerability..48
8.1.4 Threat Event Description..48
8.1.5 Outcome..48
8.1.6 Organizational Units / Processes Affected..49
8.1.7 Potential Mitigating Strategies / SCRM Controls..49
8.2 Scenario: Devices that Don't Auto-Update Firmware (Imbedded Spinal Cord Stimulator with a Hand-Held Controller)..49
8.2.1 Background..49
8.2.2 Threat Source..49
8.2.3 Vulnerability..50
8.2.4 Threat Event Description..50
8.2.5 Outcome..50
8.2.6 Organizational Units / Processes Affected..50
8.2.7 Potential Mitigating Strategies / SCRM Controls..50
8.3 Scenario: Mishandling of Critical or Sensitive Information..50
8.3.1 Background..50
8.3.2 Threat Source..50
8.3.3 Vulnerability..51
8.3.4 Threat Event Description..51
8.3.5 Outcome..51
8.3.6 Organizational Units / Processes Affected..51
8.3.7 Potential Mitigating Strategies / SCRM Controls..51
8.4 Scenario: Lack of Asset Visibility and Vulnerability Exploitation..51
8.4.1 Background..51
8.4.2 Threat Source..51
8.4.3 Vulnerability..52
8.4.4 Threat Event Description..52
8.4.5 Outcome..52
8.4.6 Organizational Units / Processes Affected..52

8.4.7 Potential Mitigating Strategies / SCRM Controls 52
8.5 Scenario: ICT Devices with Default Passwords 53
8.5.1 Background 53
8.5.2 Threat Source 53
8.5.3 Vulnerability 53
8.5.4 Threat Event Description 54
8.5.5 Outcome 54
8.5.6 Organizational Units / Processes Affected 54
8.5.7 Potential Mitigating Strategies / SCRM Controls 54
8.6 Scenario: Incorrect Privilege Settings, Authorized Privileged User, or Administrator Erroneously Assigns User Exceptional Privileges or Sets Privilege Requirements on a Resource too Low. 55
8.6.1 Background 55
8.6.2 Threat Source 55
8.6.3 Vulnerability 55
8.6.4 Threat Event Description 55
8.6.5 Outcome 55
8.6.6 Organizational Units / Processes Affected 56
8.6.7 Potential Mitigating Strategies / SCRM Controls 56
9.0 Threat Category: Compromise of System Development Life Cycle (SDLC) Processes & Tools 56
9.1 Scenario: Manipulation of Development Tools & Development Environment 56
9.1.1 Background 56
9.1.2 Threat Source 56
9.1.3 Vulnerability 57
9.1.4 Threat Event Description 57
9.1.5 Outcome 57
9.1.6 Organizational Units / Processes Affected 57
9.1.7 Potential Mitigating Strategies / SCRM Controls 57
9.2 Scenario: Compromised/Infected System Images 58
9.2.1 Background 58
9.2.2 Threat Source 58
9.2.3 Vulnerability 58
9.2.4 Threat Event Description 58
9.2.5 Outcome 58
9.2.6 Organizational Units / Processes Affected 59
9.2.7 Potential Mitigating Strategies / SCRM Controls 59
9.3 Scenario: Introduction of Vulnerabilities into Software Products from Open Source 59
9.3.1 Background 59
9.3.2 Threat Source 59
9.3.3 Vulnerability 60
9.3.4 Threat Event Description 60
9.3.5 Outcome 60
9.3.6 Organizational Units / Processes Affected 60
9.3.7 Potential Mitigating Strategies / SCRM Controls 60
10.0 Threat Category: Insider Threat 61
10.1 Scenario: Contractor Compromise 61
10.1.1 Background 61
10.1.2 Threat Source 61

10.1.3 Vulnerability 61
10.1.4 Threat Event Description 61
10.1.5 Outcome 61
10.1.6 Organizational Units / Processes Affected 61
10.1.7 Potential Mitigating Strategies / SCRM Controls 62
10.2 Scenario: New Vendor Onboarding 62
10.2.1 Background 62
10.2.2 Threat Source 62
10.2.3 Vulnerability 62
10.2.4 Threat Event Description 62
10.2.5 Outcome 63
10.2.6 Organizational Units / Processes Affected 63
10.2.7 Potential Mitigating Strategies / SCRM Controls 63
10.3 Scenario: Staffing Firms Used to Source Human Capital 64
10.3.1 Background 64
10.3.2 Threat Source 64
10.3.3 Vulnerability 64
10.3.4 Threat Event Description 65
10.3.5 Outcome 65
10.3.6 Organizational Units / Processes Affected 65
10.3.7 Potential Mitigating Strategies / SCRM Controls 65
11.0 Threat Category: Inherited Risk (Extended Supplier Chain) 65
11.1 Scenario: Sub-Agency Failure to Update Equipment 65
11.1.1 Background 65
11.1.2 Threat Source 66
11.1.3 Vulnerability 66
11.1.4 Threat Event Description 66
11.1.5 Outcome 66
11.1.6 Organizational Units / Processes Affected 66
11.1.7 Potential Mitigating Strategies / SCRM Controls 66
11.2 Scenario: Sub-Agency Failure to Update Enterprise Software 66
11.2.1 Background 66
11.2.2 Threat Source 66
11.2.3 Vulnerability 66
11.2.4 Threat Event Description 66
11.2.5 Outcome 67
11.2.6 Organizational Units / Processes Affected 67
11.2.7 Potential Mitigating Strategies / SCRM Controls 67
11.3 Scenario: Inheriting Risk from nth Party Supplier 67
11.3.1 Background 67
11.3.2 Threat Source 67
11.3.3 Vulnerability 67
11.3.4 Threat Event Description 67
11.3.5 Outcome 68
11.3.6 Organizational Units / Processes Affected 68
11.3.7 Potential Mitigating Strategies / SCRM Controls 68
11.4 Scenario: Mid Supply Insertion of Counterfeit Parts via Supplier XYZ to Trusted/Vetted Vendor 68

11.4.1 Background.......68
11.4.2 Threat Source.......68
11.4.3 Vulnerability.......68
11.4.4 Threat Event Description.......68
11.4.5 Outcome.......68
11.4.6 Organizational Units / Processes Affected.......69
11.4.7 Potential Mitigating Strategies / SCRM Controls.......69
12.0 Threat Category: Economic.......69
12.1 Scenario: Financial Strength of the Supplier.......69
12.1.1 Background.......69
12.1.2 Threat Source.......69
12.1.3 Vulnerability.......69
12.1.4 Threat Event Description.......69
12.1.5 Outcome.......69
12.1.6 Organizational Units / Processes Affected.......69
12.1.7 Potential Mitigating Strategies / SCRM Controls.......69
12.2 Scenario: Information Asymmetries.......70
12.2.1 Background.......70
12.2.2 Threat Source.......70
12.2.3 Vulnerability.......70
12.2.4 Threat Event Description.......70
12.2.5 Outcome.......70
12.2.6 Organizational Units / Processes Affected.......70
12.2.7 Potential Mitigating Strategies / SCRM Controls.......70
12.3 Scenario: Ownership Change.......70
12.3.1 Background.......70
12.3.2 Threat Source.......70
12.3.3 Vulnerability.......71
12.3.4 Threat Event Description.......71
12.3.5 Outcome.......71
12.3.6 Organizational Units / Processes Affected.......71
12.3.7 Potential Mitigating Strategies / SCRM Controls.......71
12.4 Scenario: Cost Volatility.......71
12.4.1 Background.......71
12.4.2 Threat Source.......71
12.4.3 Vulnerability.......71
12.4.4 Threat Event Description.......71
12.4.5 Outcome.......72
12.4.6 Organizational Units / Processes Affected.......72
12.4.7 Potential Mitigating Strategies / SCRM Controls.......72
13.0 Threat Category: Legal.......72
13.1 Scenario: Laws that Harm or Undermine American Economic Interests.......72
13.1.1 Background.......72
13.1.2 Threat Source.......72
13.1.3 Vulnerability.......73
13.1.4 Threat Event Description.......73
13.1.5 Outcome.......73

13.1.6 Organizational Units / Processes Affected 73
13.1.7 Potential Mitigating Strategies / SCRM Controls..... 73
13.2 Scenario: Legal Jurisdiction-Related Threats 73
13.2.1 Background..... 73
13.2.2 Threat Source 73
13.2.3 Vulnerability 74
13.2.4 Threat Event Description..... 74
13.2.5 Outcome..... 74
13.2.6 Organizational Units / Processes Affected 74
13.2.7 Potential Mitigating Strategies / SCRM Controls..... 74
13.3 Scenario: Legal Costs that Weaken the Financial Viability of a Company 74
13.3.1 Background..... 74
13.3.2 Threat Source 74
13.3.3 Vulnerability 74
13.3.4 Threat Event Description..... 74
13.3.5 Outcome..... 75
13.3.6 Organizational Units / Processes Affected 75
13.3.7 Potential Mitigating Strategies / SCRM Controls..... 75
14.0 Threat Category: External End-to-End Supply Chain 75
14.1 Scenario: Natural Disasters Causing Supply Chain Disruptions 75
14.1.1 Background..... 75
14.1.2 Threat Source 75
14.1.3 Vulnerability 76
14.1.4 Threat Event Description..... 76
14.1.5 Outcome..... 76
14.1.6 Organizational Units / Processes Affected 76
14.1.7 Potential Mitigating Strategies / SCRM Controls..... 76
14.2 Scenario: Man Made Disruptions: Sabotage, Terrorism, Crime, and War..... 77
14.2.1 Background..... 77
14.2.2 Threat Source 77
14.2.3 Vulnerability 77
14.2.4 Threat Event Description..... 78
14.2.5 Outcome..... 78
14.2.6 Organizational Units / Processes Affected 78
14.2.7 Potential Mitigating Strategies / SCRM Controls..... 78
14.3 Scenario: Labor Issues 78
14.3.1 Background..... 78
14.3.2 Threat Source 78
14.3.3 Vulnerability 79
14.3.4 Threat Event Description..... 79
14.3.5 Outcome..... 79
14.3.6 Organizational Units / Processes Affected 79
14.3.7 Potential Mitigating Strategies / SCRM Controls..... 79
14.4 Scenario: Influence or Control by Foreign Governments over Suppliers 79
14.4.1 Background..... 79
14.4.2 Threat Source 80
14.4.3 Vulnerability 80

14.4.4 Threat Event Description 80
14.4.5 Outcome 80
14.4.6 Organizational Units / Processes Affected 80
14.4.7 Potential Mitigating Strategies / SCRM Controls 81
14.5 Scenario: Malicious Supplier Inserts Hostile Content 81
14.5.1 Background 81
14.5.2 Threat Source 81
14.5.3 Vulnerability 81
14.5.4 Threat Event Description 81
14.5.5 Outcome 81
14.5.6 Organizational Units / Processes Affected 81
14.5.7 Potential Mitigating Strategies / SCRM Controls 82

6.0 Threat Category: Counterfeit Parts

6.1 SCENARIO: SERVICE CONTRACTS

6.1.1 Background

Service contracts that are governed by the Trade Agreements Act (TAA) and Federal Acquisition Regulation (FAR) 25.1 sometimes include network equipment as part of the contract agreement (e.g., routers and switches).

6.1.2 Threat Source

This threat is applicable across any federal agency with these types of TAA service contracts that include network equipment.

6.1.3 Vulnerability

These network components are not required to have any engineering analysis or certification before installation on the network. Therefore, this is a network category threat with potential exposure to content data or other messaging.

6.1.4 Threat Event Description

Depending on the Original Equipment Manufacturer (OEM) or supplier, a change to TAA would require products to be authenticated or certified and meet specific engineering quality assurance.

6.1.5 Outcome

In this scenario, this threat could impact intellectual properties, network, data and messaging, depending on the contract. The exposure could be functional for an unspecified period of time.

6.1.6 Organizational Units / Processes Affected

Uncertain if there has been an impact. This example provides insight to a potential exposure.

6.1.7 Potential Mitigating Strategies / SCRM Controls

Possibly blockchain technologies may represent one mitigation strategy. Additionally, perhaps IoT systems used to monitor integrity of shipments from supplier to consumer. These may work for hardware supply chain. For software, there are mechanisms that include hashed or signed code along with blockchain, etc.

6.2 SCENARIO: ASSET MANAGEMENT, SPECIFICALLY SOFTWARE ASSET MANAGEMENT (SAM)

6.2.1 Background

A recent article from Gartner lays out the entire risk assessment with regard to asset management (specifically Software Asset Management (SAM). Agencies currently have many tools managing SAM such as IBM's Big Fix (HCL, an Indian company, is planning on buying a large part of IBM's Portfolio), SCCM (Microsoft), HP Universal Discovery, BMC's Remedy, Flexera and smaller agencies using spreadsheets. The significance of this dilemma is actually trying to capture spend analytics of SAM as the data models are different most everywhere and much of the data are unstructured. The solution is not to force all agencies to move to one tool but guide them to a structured data model and develop Application Programming Interfaces (API's) to pull the data on demand. Below, we discuss the technology and business risks associated with SAM within federal agencies, and the true spend numbers is and perhaps represent the usage of API's to gather full asset management. One more thing: SAM requires more than looking at installed instances. Usage data is critical to monitor and control SAM lifecycle, out-of-date software, and patch management.

6.2.2 Threat Source

N/A

6.2.3 Vulnerability

The business and technology risks are that agencies have different data models with each of these applications and therefore the accuracy of installed software, software utilization and outdated installed software (no longer supported) is not uncommon and can be of significant risk. Many agencies count instances of installed software but does account for software utilization. As an example, consultants often need Microsoft Visio Professional and Project Professional. There are many licenses installed without usage as we keep purchasing without measuring usage. Likewise, upgrades are not maintained appropriately (e.g., Adobe Acrobat and other Adobe products). Often the license expires and eventually no longer supported and therefore becomes an operational risk.

6.2.4 Threat Event Description

These network components are not required to have any engineering analysis or certification before installation on the network. Therefore, this is a network category threat with potential exposure to content data or other messaging.

6.2.5 Outcome

Sourcing, procurement and vendor management leaders working with IT asset managers to and risks should do the following:

- Develop a business case for Information Technology Asset Management (ITAM) to obtain cross-functional, C-level support for a published ITAM mission statement and charter that sets the foundation for IT asset life cycle governance;
- Design and implement comprehensive and formal controls to assign accountability for all activities across the IT asset life cycle. Assess current controls with stakeholders, and develop a roadmap to mitigate gaps in current controls;

- Implement organizational and operational governance boards that drive standardization and collaboration, provide role clarity, and support the ITAM initiative. This will minimize potential conflicts and objections to new policies and processes;
- Developing and implementing comprehensive IT asset life cycle controls is fundamental to the success of every ITAM initiative. Yet, when Sourcing, Procurement and Vendor Management (SPVM) and ITAM leaders are tasked with doing so, they struggle to know where to begin. They often overlook critical life cycle activities, or are unclear as to who is responsible for managing the steps of the life cycle. This lack of clarity results in inadequate controls that ultimately expose organizations to unwanted risks, such as software license noncompliance, unsecured assets, and uncontrolled costs;
- SPVM and ITAM leaders must develop and publish a mandate that is supported by cross-functional executives and driven by the ITAM strategy. The mandate should detail the activities in the IT asset life cycle and require the implementation of controls throughout the life cycle that account for the management of all IT assets (e.g., hardware, software, and cloud services). For the controls to be effective, ITAM policies, processes and leadership must be placed at the core of the IT asset life cycle to orchestrate and coordinate all life cycle activities; and
- The biggest challenge across federal is to develop a common data model for asset management. This does not warrant moving to a single application, but does require critical data management to be consistent and develop the applicable API's to pull data regardless of the installed application.

6.2.6 Organizational Units / Processes Affected

All agencies, sub-agencies, resellers, OEMs, and integration services could be affected by this threat. Depending on where this data is used elsewhere, it may possibly require changes to other applications and systems.

6.2.7 Potential Mitigating Strategies / SCRM Controls

The following mitigation strategies could be implemented:

- The opportunity will reflect in excess of 20 percent savings and cost avoidance opportunities;
- Asset management alignment with critical suppliers (initially) will significantly reduce risk and compliance issues regardless of platform (e.g., desktop, server, mainframe, cloud and security exposure);
- Meaningful financial reporting and forecasting;
- Quality spend analytics;
- System integrity; and
- Build an overall IT Asset Management Catalog by Platform and a process for maintenance.

6.3 SCENARIO: YOKOGAWA ELECTRIC CORPORATION COUNTERFEIT EQUIPMENT

6.3.1 Background

Yokogawa Electric Corporation identified instances in which several customers received counterfeit EJA-110E high-performance differential pressure transmitters used to measure liquid, gas, or steam pressure, using the Yokogawa logo.

6.3.2 Threat Source

The threat of counterfeit equipment labeled as OEM is applicable across federal, state & local agencies, as well as the critical infrastructure sectors that rely on these devices. The threats could occur outside OEM distribution paths at Integrators, third parties, etc.

6.3.3 Vulnerability

Vulnerabilities exist in a supply chain that includes system integrators, shippers, and other third parties. The threat is applicable at any time and persistent within the infrastructure.

6.3.4 Threat Event Description

Counterfeit instruments were produced by unauthorized manufacturers. In addition to a lesser quality, Yokogawa reports that performance test results found that the counterfeit products “pose a serious safety risk.”

6.3.5 Outcome

In this scenario, this could impact intellectual properties, network, data, and messaging, depending on the contract. The exposure could be functional for an unspecified period of time.

6.3.6 Organizational Units / Processes Affected

There could be processes that impact the reseller or the integrator.

6.3.7 Potential Mitigating Strategies / SCRM Controls

N/A

7.0 Threat Category: Cybersecurity

7.1 SCENARIO: INCORRECT BORDER GATEWAY PROTOCOL (BGP) ROUTING

7.1.1 Background

BGP is the default protocol for exchanging routing information between Internet domains. Internet routing is designed to be resilient, and not dependent on any one organization. This presents a few inherent security problems that rely on trust of routing information. This inherent trust can make it harder to detect events such as route hijacking, route leaks, Internet Protocol (IP) address spoofing, eavesdropping, manipulation, and other harmful activities. BGP and other such routing threats can also be manifested by hackers who are not necessarily nation states, but also may be hacktivists or other non-state-affiliated actors. Route hijacking is when a route is accidentally or maliciously altered to send data traffic on an unintended route, or to an unintended destination. Further background information on BGP routing can be found here: https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/

7.1.2 Threat Source

The threat source in this scenario is a nation state, or other malicious actor that wishes to reroute or interrupt Internet traffic. Note that this threat can also manifest by accident. The impact will largely be the same, and the mitigations are also similar to malicious origins.

7.1.3 Vulnerability

Not all Internet Service Providers (ISPs) have implemented measures to ensure BGP announcements are coming from a legitimate source.

7.1.4 Threat Event Description

Users initially noticed a delay in certain Internet traffic. A traceroute that normally shows a route that takes two or three hops was now taking more than ten hops and also was routing via China. Further investigation shows a colocation company leaked over 70,000 routes to a foreign Tier 1 provider. This provider then announced these routes on to the global Internet, which redirected large amounts of Internet traffic destined for some of the largest European mobile networks through China Telecom's network.

7.1.5 Outcome

The incorrect routes were in circulation for about one hour. During this time, traffic was routed thru China. This routing gave China the opportunity to collect intelligence from this traffic. Specific consequences of this intelligence breach are unknown. Once the incorrect routes were discarded, Internet routing traffic returned to normal.

7.1.6 Organizational Units / Processes Affected

All organizations that had traffic rerouted thru China were potentially impacted. For the Service Provider, Network Operations and configuration of border routers were affected.

7.1.7 Potential Mitigating Strategies / SCRM Controls

Organizations evaluating Internet Service Providers can inquire about policies and procedures, which are intended to prevent such occurrences, as well as monitoring that is intended to rapidly detect these events. The service provider can be asked if they are a member of the Internet Society's Mutually Agreed Norms for Routing Security (MANRS) project.

This threat scenario, is addressed in:

- Communications, Security, Reliability, and Interoperability Council (CSRIC) WG 3 -- Best Practices and Recommendations to Mitigate Security Risks to Current IP-Based Protocols
- National Institute of Standards and Technology (NIST) SP 1800-14, Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation

7.2 SCENARIO: RANSOMWARE ATTACK

7.2.1 Background

Ransomware is a type of malware where the target's computer is rendered unusable, typically by locking the user out of their system or encrypting some or all of the data on their system. The attacker then demands a monetary (bitcoin, etc.) ransom so that the target can receive the key to recover their data or access their system.

7.2.2 Threat Source

Ransomware attacks are typically propagated by individuals or groups seeking monetary gain.

7.2.3 Vulnerability

This threat is one of opportunity in that the threat actor sets their ransomware code afloat in the electronic sea – typically via infected web sites and email messages – waiting for an unsuspecting target to click on the link. While there are some antivirus packages which will recognize potential ransomware, the best defense is for users to avoid opening email messages from strangers, clicking on embedded links in email messages or visiting web sites for which there is not a personal or business need.

7.2.4 Threat Event Description

Ransomware has a variety of delivery vehicles or methods. These are three general examples of how ransomware can accomplish its goals.

In this example scenario, the threat actor is attempting to pose as a government official who is making final contact with the target to work out details of pending litigation or fines against the target. The generally worded email message contains a link and the target is instructed to click on the link to access the case file so that the target can avoid potential time in court and pending fines. Clicking the embedded link then unleashes the ransomware onto the target's computer.

In this example scenario, the target is presented with screen pop-ups which indicate that malware has been found on the target's system and the target should click on the link to take defensive measures. Again, clicking on the link unleashes the ransomware onto the target's computer.

In this final example scenario, the target has either turned off their antivirus software or configured it to its minimal settings thereby rendering it ineffective. As the target surfs the web, they can be presented with content which would normally have been flagged by their antivirus software. The target clicks on the questionable content and again unleashes ransomware onto the target's computer.

In each of the three example scenarios, above, there generally was not a named or intended target but rather just a wait-and-see who clicks on the infected link. Having said that, ransomware messages could be directed at organizations in general (companies, hospitals, government agencies) but again waiting to see if anyone will take the bait.

7.2.5 Outcome

If the threat actor is successful, the target is now presented with a dilemma; should they pay the ransom risking that the threat actor will not provide the key, or does the target attempt to recover their data from system back-ups, which could result in losing any data since the last back-up? Given that most times the ransom is to be paid using bitcoin or similar digital currency, the money leaves no audit trail.

If the target should pay the ransom, the threat actor could lock or encrypt the system again in the future seeking additional ransom payments. Most experts recommend that ransomware payments not be made, and the organization rebuild their system(s) from data back-ups.

7.2.6 Organizational Units / Processes Affected

Any and all parts of the organization are susceptible to ransomware attacks. Everyone who uses a computer, both professionally and privately, typically uses email and surfs the web, making everyone a potential target. Given the prevalence of outsourcing of supply chain activities, suppliers can be hit with ransomware as well thereby impacting a company's supply chain activities.

7.2.7 Potential Mitigating Strategies / SCRM Controls

While there is no single way to prevent ransomware attacks, strategies worth considering include:

- Regularly perform comprehensive backups of all critical data to offline or write-only storage on a schedule consistent with the number of transactions or data being performed on the system (e.g. how many days of data is the company willing to lose since the last back-up was performed?);
- Educate users on the potential perils of opening emails from strangers or clicking on embedded links (email or web sites);
- Keep anti-virus software active and up-to-date. Where possible, don't allow users to modify or disable anti-virus software on their company issued systems; and
- Contractual agreements should be in place with all suppliers to define liability and remediation activities should a supplier be impacted by a ransomware attack.

7.3 SCENARIO: REMOVABLE MEDIA ATTACK

7.3.1 Background

Threat Actors have utilized Removable Media to insert malware into an organization's computer systems. Removable Media such as Universal Serial Bus (USB) Thumb-Drives, Compact Discs (CDs), and floppy disks have been used. For examples of such methods and attacks see:

- Operation Buckshot Yankee: http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html
- Krebs On Security Article July 2018: https://krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/

For organizations that do not have the appropriate security controls in place, when removable media is inserted into a computer, that system can look for executable files and attempt to run those programs. This can result in malware bypassing all network perimeter defenses and getting installed on systems inside the supply chain organization.

7.3.2 Threat Source

Nation state cyber threat actors have been behind the news worthy events of these removable media attacks. Cyber criminals or cyber hacktivists could also easily use this attack method.

7.3.3 Vulnerability

The vulnerability is that there is no prevention of, or pre-scanning of the malicious removable media prior to it being installed into the internal computer system. Removable media is delivered to an employee and that media is inserted into a computer system that can be compromised by that malware contained in or on the removable media.

7.3.4 Threat Event Description

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as a nation-state sponsored threat actor.

In this example scenario, the threat actor is attempting to compromise physical security systems being manufactured by the supply chain organization. The threat actor seeks to be able to remotely monitor and control the physical security systems of the supply chain organization's customers.

In this scenario, the threat actor drops many USB Drives, containing malware into the parking lot of the supply chain vendor. The USB Drives are labeled with supply chain organization's logo and the USB Drives contain file objects that appears to be related to the supply chain vendor's business.

Employees pick up the USB Drives, carry them into the organization. Many of the employees insert the USB drives into their computers. Some employees seek to return the USB Drives, some employees are curious about the USB drive contents.

In one study,[3] 48 percent of the distributed USB Drives were inserted into the organization's computers. Once inserted the computer can autorun the malware installation program. Or, the employee can attempt to open files, some with an alluring name, thus allowing the malware to start running, become installed, and open a backdoor so that the threat actor can access that system.

[3] https://www.pcworld.com/article/3070048/how-to-keep-usb-thumb-drive-malware-away-from-your-pc.html

When the threat actor has a persistent backdoor access to one of the supply chain vendor's systems, the threat actor can continue the attack.

7.3.5 Outcome

The threat actor is successful with their mission of compromising the systems being manufactured by the supply chain organization. The supply chain organization's customers are now buying systems that can be remotely controlled by the foreign military-intelligence organization. The supply chain organization is providing software updates to their existing customers, these updates contain the malicious capabilities. Depending upon the security controls in place within the customer's environment, the attacker is now able to remotely monitor and control the customers' entire physical security systems.

Additionally, the attacker now also has a foot hold in each of the supply chain organizations customer's networks. This can enable the attacker to launch additional attacks into each of those organizations.

7.3.6 Organizational Units / Processes Affected

The supply chain organization is compromised, the attacker has the ability to move freely within their network and systems. The company's products have been compromised; therefore, their customers are also potentially affected. The compromised physical security system is now a platform from which the attacker can begin to attack each organization where their security system in installed.

7.3.7 Potential Mitigating Strategies / SCRM Controls

The buyer organization, conducting this analysis, would evaluate:

- The extent to which potential supplier organizations protect themselves from removable media type attacks;
- The extent to which the organizations are connected electronically;
- The extent to which the supply chain organization has mature security-focused software development and distribution practices; and
- Internal security controls, such as micro segmentation, so that such a compromised system would not be able to communicate outside of the organization.

This threat scenario, removable media, is addressed in:

- NIST Special Publication (SP) 800-53 Rev 4 Security Control: Media Protection.
- NIST SP 800-161 [Supply Chain Risk Management Practices for Federal Information Systems and Organizations] references NIST SP 800-53 Rev 4 Security Control: Media Protection.

7.4 SCENARIO: RESOURCE DEPLETION – UNINTENTIONAL/ACCIDENTAL SHUTDOWN

7.4.1 Background

Unintentional or accidental resource depletion is a non-adversarial threat resulting from system misconfigurations or lack of resource planning. System events resulting in resource depletion or accidental shutdown may vary from misconfiguration of information systems and network connectivity to improper software updates to production environments.

Organizations operating without the appropriate security controls in place will experience regular system and network outages inadvertently caused by uncontrolled and unmanaged changes to their environments. This will cause a reduction in the organizations overall systems and network availability.

7.4.2 Threat Source

The threat source in this scenario is internal and is also non-malicious.

7.4.3 Vulnerability

The vulnerability is the lack of, (or lack of enforcement of) change management and configuration management policies and procedures within the organization.

7.4.4 Threat Event Description

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as an internal employee with non-malicious intentions.

In this scenario, the supply chain organization recently hired a new network engineer who identified some inefficiencies in the existing network configurations. The network engineer updates the system routing configurations and applies the updates to the production network without recording the updated configurations.

7.4.5 Outcome

The internal employee unintentionally caused an accidental shutdown crippling the supply chain organization's enterprise creating a negative impact on the supply chain organization and possibly their client organizations.

7.4.6 Organizational Units / Processes Affected

The supply chain organization may experience productivity inefficiencies caused by system or network outages possibly impacting their ability to support or deliver on their contracts. The supply chain organization's customers may also experience impacts to their existing operations through system, service availability, or product supply.

7.4.7 Potential Mitigating Strategies / SCRM Controls

The buyer organization, conducting this analysis, would evaluate:

- The presence of Configuration Management policies and procedures that are in place and actively enforced;
- Assess the overall impact of vendor system or network outages will have on the organizations operations; and
- Assess the overall impact of vendor system or network outages will have on the vendors' ability to meet contractual requirements.

This threat scenario, Resource Depletion/Unintentional Shutdown, is addressed in:

- NIST SP 800-53 Rev 4 Security Controls: Configuration Management, System and Information Integrity
- NIST SP 800-161 [Supply Chain Risk Management Practices for Federal Information Systems and Organizations] references NIST SP 800-53 Rev 4 Security Control: Configuration Management, and System and Information Integrity.

8.0 Threat Category: Internal Security Operations and Controls

8.1 SCENARIO: POOR ACCESS CONTROL POLICY

8.1.1 Background

An organization has a small legacy network, which has been maintained over a period of 10+ years but has not been assessed for risk or security threats in quite some time. The network is mostly static in nature, in both configuration and system level/type (OS, patch, function, applications, etc.). Over that period, the team responsible for monitoring and managing the security of this network has changed several times, with no update or re-check of policies and procedures.

The organization has decided to perform some routine network checks prior to upgrading other portions of the infrastructure and has called in a pre-existing vendor to verify systems and configurations.

8.1.2 Threat Source

The systems involved are part of legacy wireless infrastructure which still routes traffic in certain areas and is also available as fallback for emergency or backup situations.

While the current infrastructure has been through audits and assessments over time, the legacy infrastructure has largely been signed off as status quo.

8.1.3 Vulnerability

While the network routes a relatively small amount of traffic, it does have access to a large amount of subscriber information that is maintained for the current infrastructure. The systems control access to sensitive user data, Domain Name System (DNS) function and routing of user traffic in, out, and through the legacy network.

8.1.4 Threat Event Description

Due to weak access control policies, years-old user accounts from the equipment vendor are still functional. Some of these user accounts allow root or privileged access and are not uniquely identifiable as belonging to an individual or even to a certain company. The credentials for these accounts have become compromised and a malicious attacker has used them to gain access to the legacy network, where additional attacks can be sourced from.

8.1.5 Outcome

The following illustrates some of the weaknesses exposed in an attack chain that could be sourced from this supplier:

- Some equipment is accessible directly from the enterprise network, not via a firewall or Demilitarized Zone (DMZ);
- User accounts are not uniquely identifiable, reviewed or changed;
- User sessions are not controlled and vulnerable to typical brute force account access methods; and
- Potential violations of user access are not alerted.

Given the above factors, an attack would not only likely be successful but also would go undetected for a long time unless service was otherwise impacted (e.g. user traffic stopped passing or was degraded). Simple dictionary or brute force attacks would likely be successful due to access control and account management policies. Thus, theft or manipulation of data, either through man-in-the-middle or exfiltration would be quite possible. In addition, other defenses or mitigations set up elsewhere in the network could be negatively impacted or changed from within.

8.1.6 Organizational Units / Processes Affected

N/A

8.1.7 Potential Mitigating Strategies / SCRM Controls

Proper access control means protection of system resources against unauthorized access; a process by which use of system resources (e.g. executable programs, network configuration data, application file systems, network databases etc.) is regulated according to a security policy and is permitted only to authorized entities (users, programs, processes or other systems) according to that policy.

Authentication and authorization are basic security methods, which provide means to ensure the identity of users and limit their use of network resources to predefined activities or roles. They can thus be used to protect network operators against any unauthorized use of the network's services.

Furthermore, user authentication provides a basic mechanism for logging and auditing the management activities, which makes it possible to track activities afterwards. Providing each user with a unique user Identification (ID) and password together with a certain profile (privilege level) makes it possible to limit user's access to only those management activities they require in order to perform their task.

Enforcing the strong password selection, password aging (which enforces the users to change their passwords at predefined intervals), two-factor authentication, and the encryption of the files containing the user ID and password data (to prevent unauthorized users to obtain sensitive data) provide additional security.

It is also recommended to implement restrictions on the rate of login attempts, concurrent login attempts, and lockout periods for incorrect login attempts and monitored alerts for incorrect login attempts.

Security event logs or audit trails are of fundamental importance to an operator in detecting malicious activities by defining the indicators of such behavior. The log also establishes accountability for malicious users committing internal fraud or sabotage. The security event logging should be compliant to open standards to permit the administrator to perform archival and analysis of logs and for post-incident evidence gathering and investigation.

The first step to detect harmful activities is to know the indicators for such behavior. The earlier such an activity is detected, the more time is left to take appropriate countermeasures.

8.2 SCENARIO: DEVICES THAT DON'T AUTO-UPDATE FIRMWARE (IMBEDDED SPINAL CORD STIMULATOR WITH A HAND-HELD CONTROLLER)

8.2.1 Background

Failing to update your software doesn't just mean you won't have the latest version, it means you could be exposed to major security vulnerabilities that could also affect your physical wellbeing. There's medical technology today that allows patients to control their comfort levels by carrying a hand-held device to monitor and control implantable medical devices. After numerous, unsuccessful surgeries, a patient received a surgically implanted spinal cord stimulator to address years of chronic back pain. The stimulator tricks the brain to thinking the pain is gone.

8.2.2 Threat Source

The unauthorized individuals potentially accessing the device and changing the setting that control and monitor the comfort level of a patient. The hacker could turn the controller completely off making it impossible for the patient to active the device and receive the benefits provided by the device to manage pain. As defined - a threat is the potential for a threat source to successfully exploit a vulnerability.

8.2.3 Vulnerability

Hand-held devices don't auto-update and requires live conversation with a help desk and, in some instances, a trip to the patient's health care provider must take place to update the firmware and sync the device.

8.2.4 Threat Event Description

Unauthorized individuals accessing the device and changing the settings that control/monitor the comfort level of a patient. The hacker could turn the controller completely off making it impossible for the patient to activate the device and receive the benefits provided by the device to manage pain. Conversely, the hacker could turn the controls up or down making the pain encountered by the patient intolerable.

8.2.5 Outcome

Since it doesn't appear to allow hackers to gain access to a patient's medical/personal history, the primary threat is controlling the device itself, which is some instances where the imbedded device may be something other than a spinal cord stimulator (i.e. pacemaker) could be life altering.

8.2.6 Organizational Units / Processes Affected

N/A

8.2.7 Potential Mitigating Strategies / SCRM Controls

- To mitigate the seriousness of such an attack, patients who have an imbedded device that require updates from time to time should ensure that their contact information is kept up to date with the manufacturer of the medical device, as well as their health care providers so that the patient can be notified when an update to a device is required;
- Periodically, contact the manufacturer of the device for firmware updates; and
- Make regular appointments with healthcare provider to ensure the device is working properly.

8.3 SCENARIO: MISHANDLING OF CRITICAL OR SENSITIVE INFORMATION

8.3.1 Background

An energy company supplier, Griffon Power, routinely handles marketing and technical information on industrial components used throughout their network. These are sometimes internal in nature but are generally marked as such. Recently, a small team within the company reviewed confidential external information from a domestic supplier on parts that were proposed for new turbines. These documents were highly sensitive in nature and shared under a Non-Disclosure Agreement (NDA).

8.3.2 Threat Source

As part of the project analysis, the team set up a shared network drive to distribute and review information. All information related to the project was stored within this folder, which was only accessible internally. Griffon Power ultimately decided not to go forward with the new turbine offering and moved on with other business. About a year later, as part of a network cleanup and upgrade effort, network storage was decommissioned and sold off to an offshore company for parts.

Much of the NDA-level information shared between Griffon Power and the potential supplier has not been properly handled and is now exposed to a third party company.

8.3.3 Vulnerability

Not having a process, to properly decommission network storage which was eventually sold off to an offshore company for parts.

8.3.4 Threat Event Description

Proprietary information on the inner workings and specialty parts of turbines that are used throughout energy companies has been made available and sold on the dark web. This could be used for economic or blackmail purposes or by foreign competitors to gain an unfair advantage in the market.

8.3.5 Outcome

Some of the weaknesses exposed in Griffon Power's policies on the handling of data are:

- Failure to wipe data that is no longer used;
- Failure to classify data – then handle and protect according to the classification;
- Failure to implement document-level encryption for sensitive data; and
- Failure to audit systems prior to decommissioning.

8.3.6 Organizational Units / Processes Affected

N/A

8.3.7 Potential Mitigating Strategies / SCRM Controls

Data management policies can have a broad range of useful steps that could prevent such risks in this scenario. All data should be classified according to its intended use, who is allowed to access it, and if or how it can be shared. In addition, data tags could be set according to whether it is Public, Limited Release, Internal or Confidential (for example). Depending on how the data are classified, it may need to be encrypted and have access to the data controlled and monitored.

Separately, companies should have a process and policy for decommissioning equipment and perform regular audits before any such equipment is released, sold or distributed. At a minimum, any non-Public data should be removed from any systems; in most cases, it is advisable to perform a complete wipe of data or destruction of storage devices to a sufficient level that data cannot be recoverable later.

8.4 SCENARIO: LACK OF ASSET VISIBILITY AND VULNERABILITY EXPLOITATION

8.4.1 Background

An organization in the supply chain lacks visibility into the range and numbers of assets connecting to its network. Further, this organization only scans for vulnerabilities on an annual basis, as part of a compliance requirement. The organization also fails to plan and prioritize its vulnerability mitigation practices.

8.4.2 Threat Source

Many high-profile incidents, including the Equifax breach and WannaCry, could have been prevented through better cyber hygiene. Fifty-seven percent of enterprises that experienced a breach in the past two years state that a known, unpatched vulnerability was the root cause.[4]

[4] "State of Security Response," Ponemon/ServiceNow, 2018

The discovery and disclosure of vulnerabilities continue to grow in volume and pace. In 2018 alone, an average of 45 new vulnerabilities were published every single day, for a total of 16,500, up from 15,038 in 2017.[5]

With 59 percent of all vulnerabilities in 2018 rated as Critical or High severity, security organizations are challenged to determine which vulnerabilities truly represent a risk and prioritize the most critical vulnerabilities to maximize limited remediation resources. After all, the proportion of Common Vulnerabilities and Exposures (CVEs) with a publicly available exploit was seven percent in 2018, down one percentage point from 2017.

8.4.3 Vulnerability

The vulnerability in the scenario is that the organization in the supply chain lacks visibility into the range and numbers of assets connecting to its network.

8.4.4 Threat Event Description

As more devices are connected, the attack surface expands, often in unexpected places, such as building management systems and Close-Circuit Televisions (CCTVs). These systems perform multiple functions, such as managing access to specific doors, controlling door alarms, creating the photo IDs that allow facility access and monitoring for access.

Coupling together three vulnerabilities in the past year, an attacker could setup a Zoom video conference with any target at the organization. Once connected, the attacker can control the attendee's screen by exploiting a vulnerability in Zoom[6] allowing them to download and install malware on the target's computer.

With access to the target computer, the attacker can then exploit the building management system[7] allowing physical access to the building. Now that the attacker can access the facility, the last step is to ensure the CCTV does not record their intrusion by exploiting the CCTV system.[8] In this scenario, an attacker could exploit software vulnerabilities to gain administrator rights, enabling them to create fraudulent ID's, disable door locks and alarms, access sensitive authorized user data and delete video footage.

8.4.5 Outcome

Building management contractors, just like IT managers, must consider cyber risk associated with all computer systems and networks within their scope of responsibility. Often times, building management systems and CCTV are outside the control or purview of organization IT departments. A disciplined Vulnerability Management program, by which the organization can track, assess, and remediate known vulnerabilities across their entire attack surface in a timely manner, before they can be exploited is a must.

8.4.6 Organizational Units / Processes Affected

N/A

8.4.7 Potential Mitigating Strategies / SCRM Controls

- Identify business operations and assets most vulnerable to cyber-attacks, to include third party, Operational Technology (OT) and IoT assets; for many organizations, the most critical assets are those that have the highest monetary value attached to them; for the government, this may be those deemed most mission critical;

[5] Primary Research, Tenable Vulnerability Intelligence
[6] https://www.tenable.com/press-releases/tenable-research-discovers-vulnerability-in-zoom-that-could-lead-to-conference
[7] https://www.tenable.com/blog/multiple-zero-days-in-premisys-identicard-access-control-system
[8] https://www.tenable.com/press-releases/tenable-research-discovers-peekaboo-zero-day-vulnerability-in-global-video

- Utilize continuous threat intelligence to prioritize remediation efforts in light of the overwhelming number of new vulnerabilities; organizations should use contextual factors including asset criticality and whether there are exploits available for specific vulnerabilities, in prioritization;
- Frequent scanning and reporting is critical, because out-of-date data can be just as damaging as inaccurate data. The Center for Internet Security (CIS) Control 3.1 recommends automatically scanning all systems on a weekly or more frequent basis;
- Organizations need to make sure their reporting is aligned with their patch remediation cycle so that reporting and updates are relevant;
- Identify the security gaps and opportunities to reduce complexity in the IT security infrastructure that leave organizations vulnerable to cyber-attacks;
- Measure the value of responding to vulnerabilities through automation and machine learning; and
- Utilize IT security staff and resources to improve the efficiency of vulnerability management.

8.5 SCENARIO: ICT DEVICES WITH DEFAULT PASSWORDS

8.5.1 Background

All ICT devices ship with default passwords, not changing the administrator password can result in the attacker to easily identify and access ICT systems. It is imperative to change default manufacturer passwords and restrict network access to critical and important systems.

8.5.2 Threat Source

One of the first things a hacker checks is whether the default account and password are enabled on a device. Websites such as www.defaultpassword.com list the default credentials, old and new, for a wide variety of devices:

- Routers, access points, switches, firewalls, and other network equipment
- Databases
- Web applications
- Industrial Control Systems (ICS) systems
- Other embedded systems and devices
- Remote terminal interfaces like Telnet and SSH
- Administrative web interfaces
- ERP systems

In 2014, Trustwave released the results of an analysis of 691 data breaches and concluded that one third were due to weak or default passwords. In 2018, it was reported that less than 8 percent of analyzed breaches were due to weak or default credentials. While the trend suggests that password security is improving, it remains crucial to have a process in place for dealing with new equipment which may still be configured with the manufacturer’s passwords.

8.5.3 Vulnerability

Devices ship with default passwords, not changing the administrator password can result in the attacker to easily identify and access ICT systems. It is imperative to change default manufacturer passwords and restrict network access to critical and important systems.

8.5.4 Threat Event Description

A small ISP has been breached by an attacker that has gained access to the enterprise network through a router with the factory default password.

8.5.5 Outcome

The attacker with knowledge of the password and network access to a system can log in, usually with root or administrative privileges. Further consequences depend on the type and use of the compromised system. Examples of incident activity involving unchanged default passwords include:

- Internet Census 2012 Carna Botnet distributed scanning;
- Fake Emergency Alert System (EAS) warnings about zombies;
- Stuxnet and Siemens SIMATIC WinCC software;
- Kaiten malware and older versions of Microsoft Standardized Query Language (SQL) Server;
- Secure Shell (SSH) access to jailbroken Apple iPhones;
- Cisco router default Telnet and enable passwords; and
- Simple Network Management Protocol (SNMP) community strings.

8.5.6 Organizational Units / Processes Affected

N/A

8.5.7 Potential Mitigating Strategies / SCRM Controls

- To reduce the risk of security breaches through default credentials which have been left configured on network devices, it’s best to implement a process to change the passwords, and if possible account names, when new equipment is installed.
- Identify software and systems that are likely to use default passwords. Regularly perform vulnerability network scans to identify systems and services using default passwords. Additionally, utilize good password management including:
  - Change Default Passwords - Change default passwords as soon as possible and absolutely before deploying the system on an untrusted network such as the Internet. Use a sufficiently strong and unique password. See the United States -Computer Emergency Readiness Team (U.S.-CERT) Security Tip ST04-002 and Password Security, Protection, and Management for more information on password security;
  - Use Unique Default Passwords - Vendors can design systems that use unique default passwords. Such passwords may be based on some inherent characteristic of the system, like a Media Access Control (MAC) address, and the password may be physically printed on the system;
  - Use Alternative Authentication Mechanisms - When possible, use alternative authentication mechanisms like Kerberos, x.509 certificates, public keys, or multi-factor authentication. Embedded systems may not support these authentication mechanisms and the associated infrastructure;
  - Force Default Password Changes - Vendors can design systems to require password changes the first time a default password is used. Recent versions of DD-WRT wireless router firmware operate this way; and
  - Restrict Network Access - Restrict network access to trusted hosts and networks. Only allow Internet access to required network services, and unless absolutely necessary, do not deploy systems that can be directly accessed from the Internet. If remote access is required, consider

using Virtual Private Network (VPN), SSH, or other secure access methods and be sure to change default passwords.

- Vendors can design systems to only allow default or recovery password use on local interfaces, such as a serial console, or when the system is in maintenance mode and only accessible from a local network.

8.6 SCENARIO: INCORRECT PRIVILEGE SETTINGS, AUTHORIZED PRIVILEGED USER, OR ADMINISTRATOR ERRONEOUSLY ASSIGNS USER EXCEPTIONAL PRIVILEGES OR SETS PRIVILEGE REQUIREMENTS ON A RESOURCE TOO LOW

8.6.1 Background

Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.

8.6.2 Threat Source

Access controls that define specific sets of privileges linked to individuals are a fundamental security practice. However, these same principals are not always applied to the most sensitive access of all; high-privilege access administrative accounts that have massive control over business-critical IT functions.

High-privilege access may be the most sensitive aspect of IT. Administrative accounts have the ability to make widespread changes to IT systems on which the business may depend. If misused, these capabilities can cause extensive damage ranging from security threats and compliance violations to incidents that tarnish the reputation of the business itself.

8.6.3 Vulnerability

The vulnerability is that the company until recently had no formal Information Security Policy or related procedures. There has been no policy for assigning system privileges, leading to many users having administrative or super user system privileged access which are not required for their current job. In this scenario, a user was granted root access to a UNIX system, in which the operating system does not apply access controls to the user root. That user can terminate any process and read, write, or delete any file.

8.6.4 Threat Event Description

Acme Packet is a midsized manufacturing company which has doubled its enterprise product offering and number of employees. When the company first started, it had less than 25 employees, many of which had multiple responsibilities. One example includes the office manager also serving as their IT department. Additionally, the company until recently had no formal Information security policy or related procedures. There has been no policy for assigning system privileges, leading to many users having administrative or super user system privileged access which are not required for their current job.

In this scenario, a user was granted root access to a UNIX system, in which the operating system does not apply access controls to the user root. That user can terminate any process and read, write, or delete any file.

8.6.5 Outcome

The scenario above presents multiple risks to the supply chain ranging from insider risks to cyber espionage. Additionally, the easiest way for a cyber-attacker to gain access to sensitive data is by compromising an end user's identity and credentials. Things get even worse if a stolen identity belongs to a privileged user, who has even broader access, and therefore provides the intruder with *the keys to the kingdom*. By leveraging a *trusted* identity, a hacker can operate undetected, gaining access to sensitive data and system access with little or no indications to the attack.

8.6.6 Organizational Units / Processes Affected

N/A

8.6.7 Potential Mitigating Strategies / SCRM Controls

- Conduct a security review of all users physical and system access adjusting user access to least privileged access, the minimum access needed to perform the job.
- Establish an Information Security Policy based off industry standards and best practices
- Deploy and Privileged Access Management (PAM) system for monitoring and protection of super user accounts. This is one of the most important aspects of Identity and Access Management, and cybersecurity at large today. With a PAM solution in place, an organization can dramatically reduce the risks discussed above.
- The Best Practices for Privileged Access Management utilize the Four Pillars of PAM. Gartner outlines key challenges and makes clear recommendations that emphasize the critical role of people, processes and technology in effectively mitigating PAM risk and making purchase decisions, including:
    - Track and Secure Every Privileged Account;
    - Govern and Control Access;
    - Record and Audit Privileged Activity; and
    - Operationalize Privileged Tasks.

9.0 Threat Category: Compromise of System Development Life Cycle (SDLC) Processes & Tools

9.1 SCENARIO: MANIPULATION OF DEVELOPMENT TOOLS & DEVELOPMENT ENVIRONMENT

9.1.1 Background

Both hardware (printed circuit boards and computer chips) and software (source or object code and firmware) are highly reliant upon automated development tools. A Printed Wiring Board (PWB) (the circuit board to which components are soldered) is composed of hundreds, if not tens of thousands of circuit traces and component connections. A much smaller instance of this is the computer chip which can contain thousands of transistors and other elemental circuit components. Likewise, on the software side, computer code in its source form can constitute thousands or millions of lines of instructions, and often integrates dozens of third-party components. Once compiled, this can reach megabytes of binary code.

Given the complexity of both hardware and software development processes, threat actors may seek to introduce vulnerabilities into the hardware or software through development processes or tools, or by compromising the development environment.

9.1.2 Threat Source

Manipulation of development tools and development environments can come by way of a variety of different threat actors: nation state, organization or individual (outsider or insider).

9.1.3 Vulnerability

The threat actor may use the complexity of the hardware or software itself (thousands of circuit traces or lines of source code) to help cover their tracks. If the development environment is not set up and managed correctly with all developers observing the accepted organizational rules-of-the-road and adopting secure configurations and controls, threat actors can use the complexity to their advantage (e.g. lax check-out check-in procedures, non-existent or minimal revision processes, unprotected code repositories, etc.). Misconfigured or unpatched anti-virus software was unable to detect the infected software running the factory machines implanted from the USB drive.

9.1.4 Threat Event Description

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as an individual threat actor in the first case and a nation state in the second case.

In this example scenario, the threat actor is a hardware Research & Development (R&D) engineer of the company. He or she reconfigures a computer-assisted design (CAD) system so that he or she can work remotely from home. The company's IT department was not consulted when a hole was created in the company firewall. While the employee was well-intentioned and took it upon him or herself to do the work, a vulnerability has now been introduced into the company.

Additionally, in this example scenario, the threat actor is a rogue nation state. After surveilling the target company via the Internet for some time, the threat actor has found an unpatched vulnerability allowing remote access to the company's development environment housing source code. The threat actor can now decipher the source code to learn the inner workings of a particular product, thereby stealing the Intellectual Property (IP*) for their own use or profit.

9.1.5 Outcome

In the first scenario, the well-intentioned employee has created a vulnerability in the development tools which is just waiting to be exploited by a bad actor (nation state, organization or individual). The vulnerability is eventually exploited, and the company finds itself under attack.

In the second scenario, not keeping systems patched and knowing where vulnerabilities can exist has led to the company's IP* being stolen, thereby leading to a company's loss of market share and dominance in a particular market sector.

9.1.6 Organizational Units / Processes Affected

In both of these scenarios, the company who owns the development tools and the development environment is directly impacted. R&D and manufacturing operations both rely upon the development tools and associated development environment for the data they contain. If IP* has been stolen, long term viability of the company may be at stake.

9.1.7 Potential Mitigating Strategies / SCRM Controls

Preventing the manipulation of a company's development tools and development environment can benefit from the following:

- Access controls and identity and authentication management controls must be in place for all development tools (hardware and software) and for the broader development environment. Only those people with a need to access the tools and data should be granted access, no more. When appropriate, enforce segregation of duties on hardware or software projects such that a developer (hardware or software) can only access their particular area of the design. Where possible, use identity management and change management tools to track changes made to the project;

- Providing external access (outside the company firewall) to any tools or data must be done in coordination with the IT department or equivalent function within the company;
- Keep all system and tool patches up-to-date; and
- Observe good SDLC practices in the development environment (check-out check-in, revisions, etc.) and remove old code when it is no longer needed.

9.2 SCENARIO: COMPROMISED/INFECTED SYSTEM IMAGES

9.2.1 Background

To gain economies of scale, electronic products are typically assembled and programmed on an assembly line. In this case, the first unit looks like the second unit, which looks like the nth unit. One down side to this approach is that when infected code is found in one unit (infected via software download to rotating media, embedded firmware, etc.), ALL units will contain this infected code. Having compromised or infected system images on the factory floor can become a huge problem for the manufacturer.

9.2.2 Threat Source

Compromise or infection of system images can come by way of a variety of different threat actors: nation state, organization or individual (outsider or insider).

9.2.3 Vulnerability

The working assumption on the factory floor is that everything is good until an issue is discovered. Automated hardware test systems can be quite adept at finding hardware issues (parts out of spec/tolerance, parts loaded incorrectly, wrong speed grade of parts used, etc.). What is more elusive is the ability of the factory floor equipment to find compromised or infected software. Hardware can be touched and physically examined. Software is 1's and 0's and must be examined using software tools which have been tuned to look for specific flaw, compromise, or infection…a more challenging task!

9.2.4 Threat Event Description

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as an individual threat actor.

In this example scenario, the threat actor is an external actor who develops and distributes malware implanted on a desktop Personal Computer (PC). A hardware engineer responsible for products being manufactured on the adjacent factory floor inserts a USB thumb drive into his or her desktop PC, copies some required files onto the drive and removes it from the PC. The engineer then enters the factory floor where he or she inserts the thumb drive into one of the factory floor control systems.

Unknowingly he or she has transferred a virus from the desktop PC to the factory floor. The virus, which may include code enabling the threat actor to manipulate or sabotage an infected product, now finds its way onto the product flowing down the manufacturing line. Soon those infected products are shipped to customers around the world.

9.2.5 Outcome

After the product is delivered to the customer, they turn on the new piece of equipment, the customer then runs an anti-virus program only to discover the new unit is infected. The customer contacts the manufacturer, demanding why they are receiving infected product. This puts the manufacturer into emergency mode with all hands on deck to track down the source of the virus…is this a one-off situation? Are other customers seeing this issue? Was the product tampered with in route to the customer? Many questions need to be answered in very short time!

9.2.6 Organizational Units / Processes Affected

While the end user customer is the first to be impacted with a compromised or infected system image, ultimately it is the manufacturer who bears the brunt of the impact. The two questions that need immediate answering are *how* and *where* was the code compromised or infected? Once that is determined, the conversation then turns to mitigation strategies to prevent further compromise or infection and how to address all the units currently in other customers' hands which contain the same compromise or infected system image (this includes any potential announcement to be made to the press). These will be all hands on deck activities from both R&D engineers and the factory floor team.

9.2.7 Potential Mitigating Strategies / SCRM Controls

There is no single method of preventing compromised or infected system images from finding their way on the factory floor. Prevention strategies should include the following:

- Use hashes or other analytical tools to confirm that the system image on the factory floor master system has not been changed/compromised. Depending upon the effort involved, this should be performed at least once daily; before and after each shift would be preferred;
- Create a list of all files required on the customer product. Periodically check the file content of the factory floor systems against this list to ensure additional files have not been placed on the factory floor system. These additional files could cause serious issues once the equipment is installed at the customer site;
- Restrict the use of USB thumb drives and other removable media on the factory floor. If removable media must be used (either to move information onto or off of the factory floor or as part of the manufacturing process), purchase the media from reputable suppliers. Scan the removable media with anti-virus software when entering and leaving the factory floor;
- System images can be compromised or infected by other methods, such as a threat actor accessing the factory floor systems via an unpatched system or network vulnerability;
- Ensure all system and network patches are installed and anti-virus software is up-to-date;
- Ensure that appropriate physical access controls are in place for the factory floor. The factory floor should be accessed only by those individuals who have need to do so; and
- Ensure that any new or updated system images being loaded onto the factory floor manufacturing systems have been thoroughly scrubbed to ensure viruses are not present in the code or file set.

9.3 SCENARIO: INTRODUCTION OF VULNERABILITIES INTO SOFTWARE PRODUCTS FROM OPEN SOURCE

9.3.1 Background

Modern software development practices often involve the integration of open source components into a larger piece of software, and complex software products or services may integrate dozens or even hundreds of such components. Open source libraries provide developers with ready-made, community-vetted code to perform discrete functions used in larger software products and services. As such, open source code can be a huge time saver for any programmer who is typically faced with seemingly impossible development deadlines. In some cases, the use of open source code can significantly reduce software development times.

9.3.2 Threat Source

Vulnerabilities introduced by the use of open source code are typically done by individual actors, but can also be introduced by organization or nation-state actors.

9.3.3 Vulnerability

The very nature of open source code is that anyone can typically view and manipulate the source code to meet their needs (some licensing requirements may apply). Given this openness, peer review is relied upon to keep the code clean and free of malware. An experienced and determined software engineer could hide a few lines of malicious code in the open source, intending that it goes unnoticed.

9.3.4 Threat Event Description

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as an individual threat actor.

In this example scenario the threat actor injects a few lines of malicious code into some commonly used open source code. A software project team, under severe time constraints, picks up and uses the infected open source code and the development team's tools for vetting and testing the component do not detect the malicious code. Unknowingly they have introduced a vulnerability into their software code.

9.3.5 Outcome

The vulnerability has gone undetected in the software team's code and the threat actor is able to compromise the software through the inserted vulnerability. The resulting effect on the code and ultimately the end customer can take a variety of forms, from being annoying to impacting system performance to the loss of data.

9.3.6 Organizational Units / Processes Affected

The end user customer is directly impacted in whatever way the injected code manifests itself. Since much of the open source code is ultimately compiled into larger pieces of code, it will be difficult for the customer to isolate and eliminate the issues introduced by the rogue code.

Once reported to and isolated by the manufacturer, eliminating the problem code will require recompilation of the source code and distribution to the customers, assuming the customers are able to download the updated object code.

9.3.7 Potential Mitigating Strategies / SCRM Controls

Strategies to help prevent the unintended introduction of vulnerabilities when using open source code include:

- Performing open source peer code reviews to help ensure the open source code is clean;
- Subject all third-party components to common software and security testing tools and practices;
- Maintain a protected source code library of pervious pieces of open source code which have been vetted and approved for use in the company. Keep the source code files up-to-date with any patches which have been issued in the open source community for that particular file. Use file integrity tools to ensure the code library is not tampered with.
- Observe all SDLC practices involving open source code. The code is only as strong as its weakest link. Cutting corners to save time or stay on schedule could cost dearly later; and
- Monitor open source vulnerability news and keep open source libraries patched and up-to-date.

10.0 Threat Category: Insider Threat

10.1 SCENARIO: CONTRACTOR COMPROMISE

10.1.1 Background

Nation-state threat actors have always utilized people to help them conduct their intelligence gathering operations. In some cases, they attempt to infiltrate people into an organization. In other cases, the threat actors attempt to compromise people already working at the organization of interest. These people might be employees or onsite contractors. In another aspect, corporate espionage by competitors can be effected via an insider.

Additionally, there are non-nation-state, ideologically driven, organizations that attempt to recruit individuals that could be onsite contract employees.

The risks presented by this type of attack are compounded when organizations outsource some of the work that needs to be accomplished. The risk is compounded because often it's the company that is hired that is screening the employees that will be onsite performing the work.

This sample threat scenario is the case where an onsite IT contractor employee is compromised, or recruited, by a threat actor and becomes an insider threat.

This scenario will not address all of the potential negative actions the insider could take. This scenario will focus on mitigating the chances that such a compromised insider, from the supply chain, can remain undetected once the compromise takes place.

10.1.2 Threat Source

The threat source, in this example, is an onsite contract employee that becomes compromised, or recruited, by a threat actor. The contract employee then becomes an onsite tool of the threat actor.

10.1.3 Vulnerability

The vulnerability in this example is the inability to detect that an employee has become compromised, or recruited, by a threat actor.

10.1.4 Threat Event Description

A full-time contract employee is providing IT Services to an enterprise. The enterprise is the target of the threat actor. The threat actor may wish to steal, change, destroy, or hold hostage data or the threat actor may wish to disrupt operations, or corrupt or sabotage a product.

The relevant threat event is the successful recruitment of the contractor individual and the fact that the individual then attempts to undertake the malicious activity.

10.1.5 Outcome

The outcome is an undetected malicious insider that is a contract IT employee, coupled with activity that the undetected malicious insider undertakes.

10.1.6 Organizational Units / Processes Affected

The affected organization is the organization that has the onsite IT Contractor working within their environment. Depending upon the specific bad activity, other potential impacts could occur for other business partners of the enterprise.

10.1.7 Potential Mitigating Strategies / SCRM Controls

The potential mitigating strategies would be an element of the Risk Management Process as described by the Risk Management Framework. See the following for more information: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

Potential Mitigating Strategies could include:

- Contractually requiring contractors to have the same background and periodic security check that employees must conform to. Additionally, the contractor company would be required to share the results of these checks with the buyer or hiring organization.
- Delivering insider awareness training to enterprise employees, and contractors, would better enable the insider-contract-employee to be identified.

10.2 SCENARIO: NEW VENDOR ONBOARDING

10.2.1 Background

Reaching out to new semiconductor companies can give manufacturers a performance or pricing edge, especially when the market has lean margins to work from and compete for government contracts.

Chips Inc., a semiconductor (SC) company used by the organization to produce military and aerospace systems, is considering a partnership with American Systems Co. to leverage their fabrication facility. This would represent a significant change in the supply chain related to a critical system element. American Systems Co. formed a task force in conjunction with Chips Inc., to help identify risks in the potential partnership and how they can be mitigated by both companies and their contractors.

10.2.2 Threat Source

American Systems Co. is concerned about the intellectual property and their patents regarding the Chips Inc. fabrication facility. They would like to monitor and control for chip over-production and mitigate loss of IP or extra chips that might end up in their competitor’s hands. These critical capabilities are currently innovative and a key driver of American Systems Co.

Additionally, Chips Inc. is located in Hong Kong and in reviewing the financial viability of the company, American Systems Co found that they receive considerable government subsidies to encourage technical sector companies in Hong Kong.

10.2.3 Vulnerability

This is a risk with regard to insiders, as Chips Inc. has had a government subsidy and may lose that subsidy which keeps the company viable.

This may result in the sale of sensitive IP that belongs to American Systems Co.

Chips provides field service teams in 15 countries to service the chips and platforms manufactured by them. Within the United States (U.S.), the field services are provided by a contractor who outsources to subcontractors in various geographical locations to provide coverage in the U.S.

10.2.4 Threat Event Description

The contractors and subcontractors all wear the same TechServices polo shirts and name badges when they are performing onsite services. Through these support contracts, TechServices personnel are able to access American Systems Co.’s field sites across the country, including sensitive or critical facilities. The contractors have access to spare parts at all times as some of the response times for customer outages have a 2 hour performance window.

10.2.5 Outcome

N/A

10.2.6 Organizational Units / Processes Affected

The risks of bringing aboard a new vendor is an important task and the challenge of working with a vendor that supports their products directly requires a more extensive vetting and monitoring.

This vendor onboarding process includes parts and components that involve sensitive American Systems Co. intellectual property. Chips Inc. has direct access to the electronic circuit design, testing and packaging aspects of American Service Co.'s intellectual property. They will have unique access to supply / demand data as they'll know how much product American Service Co.'s buys and where the company requests shipments to be delivered. Since Chips Inc. takes care of shipment and delivery of the products, they have exceptional knowledge of the processes that American Service Co.'s product use to receive, integrate and support the products they make.

Finally, Chips Inc. supports their customers' deployments of their fabricated chips and technologies by way of TechServices. TechServices is a value added service which maintains replacement parts and contains technicians on a 24/7 basis to respond to customer outages and issues very rapidly. While the parts are held separate from the technicians, Chips Inc. does provide the service and has extensive knowledge and access to American Service Co.'s sensitive operational facilities, internal processes and extensive access to spare parts, and lastly, since TechServices is contracted and subcontracted, other companies and personnel from higher risk personnel, may actually be the ones delivering services to your company, gaining access to critical facilities and having access to parts before they are installed into American Service Co.'s systems. There is likely no prohibition that TechServices can provide services to American Service Co.'s competition and may share data verbally or otherwise to their competition.

10.2.7 Potential Mitigating Strategies / SCRM Controls

A broad-based team focus and engagement strategy to work with Chips Inc. is essential to elicit all the potential risks and then develop risk mitigation strategies. Using the NIST SP 800-30 Rev. 1, and 800-171 or ISO IEC 27036 you can conduct risks assessments and perform risk management functions.

Potential Mitigating Strategies could include:

- Phasing of the onboarding of services. Initial services to fabricate chips should be developed first. Additional services provided by Chips Inc., such as TechServices can be phased in after initial risks and monitoring are in place;
- For delivery and distribution, American Service Co can keep its existing distribution center to receive deliveries and monitor parts from Chips Inc. for compliance. The common distribution center can effectively shield off much of American Service Co.'s infrastructure and operations from Chips Inc. insights;
- American Service Co can work with Chips Inc. procedures and work to update any lost or non-compliant chips and products;
- Limit American Service Co.'s, Point of Contacts (POCs) who interact with Chip Inc. from an acquisition standpoint. Make those POCs clear to Chips Inc. and give the POC's training to identify what data and types of data to share with Chips Inc.;
- Agree to security measures for transmission, encryption, storage, retention and destruction process and required paperwork of intellectual property shared to Chips Inc.;

- When American Service Co. decides to utilize support services from TechServices, American Service Co. can request TechServices employees have a background check before being allowed to participate on its contract. The same request can be done for Chips Inc. employees that interface with American Service Co.; and
- American Service Co should monitor the financial performance of Chips Inc. on a quarterly or bi-annual basis to monitor for changes in the company's financial performance or leadership changes.
- Flow-down security and risk-management policies to the supplier(s)
- Perform periodic audits of the supply chain.

10.3 SCENARIO: STAFFING FIRMS USED TO SOURCE HUMAN CAPITAL

10.3.1 Background

Nation state threat actors utilize a myriad of vectors to insert, influence, turn, or threaten company insiders into a compromising position, often resulting in the loss of a company's confidential or classified data or impact to a company's critical systems and services.

NIST defines an Insider as: One who will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the entity they work for. This threat can include damage through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of entity resources or capabilities.

While it is common for a nation state threat actor to apply leverage to an existing company insider in order to achieve a specific goal, the unwilling or untrained insider threat can often be more easily identified as compared to a planted insider. In any case, companies should have an operational Insider Threat Program (ITP) [NIST 800-53 & 800-171] wherein they employ active controls and awareness training to collect automated and manual notifications of potential insider threats.

In addition to the internal controls for the detection and prevention of insider threats, companies must also consider the insider threats stemming from their supply chain; in this scenario, the focus is the sourcing of employees, contractors, and consultants.

10.3.2 Threat Source

The threat source, in this example, is a nation state having influence over a staffing firm used by a company to source human capital. Staffing firms are often leveraged for two primarily purposes; (1) to source employee candidates, and (2) to provide skilled contractors or consultants as part of fixed-priced services.

In either case, the sourcing of candidates performed by the staffing firms can be manipulated to ensure certain qualified candidates (who are also insider threat agents) gain the first opportunities for employment. If selected for employment or contractor or consulting services, the threat agents begin to leverage access permissions to escalate privileges and acquire or disseminate data to unauthorized entities.

10.3.3 Vulnerability

The vulnerability in this example involves the partnership with a third party staffing firm who is instrumental in sourcing candidates for employment, and of which the staffing firm can be leveraged by a nation state to manipulate the recruitment and candidate sourcing to a company. In many of these cases, the staffing firm has offices around the world, while also having a recruitment or candidate database that can be accessed and modified by the staffing firm's international associates, with the intent of strategically planting insider agents into the recruitment process of a company.

Background checks can be effective for preventing the hiring of known malicious characters, but they may not detect willing insider threat agents. Also, if the staffing organization is offshore, background check policies, procedures, and mechanisms may be inadequate to appropriately vet personnel. While it is important to maintain controls that detect and stop insider threat activity, preventing the hiring an insider threat agent can help mitigate this risk. This requires the adoption of SCRM controls to be applied to staffing firms. Hardware supporting their network routers, switches and hubs had not been upgraded in five years, which exposed the firm to a vulnerability, a shortcoming or hole in the security of an asset.

10.3.4 Threat Event Description

An insider threat agent successfully navigates the hiring process and secures employment (full-time, part-time, contractor, or consultant) with the target company. The insider agent uses their authorized access to acquire confidential or classified data and attempts to escalate their privileges when needed to acquire data when access is not currently granted. The insider agent maintains a slow and undetectable process for data exfiltration. This activity could last for years without detection. When finally detected years later, the investigation found that the agent was sourced from the company's staffing firm. Background checks at the time of hire did not find anything to highlight the potential threat.

10.3.5 Outcome

Nation state extracts technology and data that allows them to influence financial markets, reverse engineer product or services, and give a tactical or competitive advantage to its cause.

10.3.6 Organizational Units / Processes Affected

The affected organization is the organization that sources candidates from the staffing firm which is had an unknown international presence. The insider agent can affect the company's competitive edge, customer market percentage, reputation, and result in financial and regulatory penalties.

10.3.7 Potential Mitigating Strategies / SCRM Controls

The potential mitigating strategies would be an element of the risk management process as described by the Risk Management Framework. See the following for more information: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

Potential Mitigating Strategies could include:

- Performing SCRM assessment on all staffing firms used to source candidates for privileged access roles; the assessment should ensure the staffing firm does not have an international database which allows remote locations to influence the candidate hire dataset for a company; and
- Perform background checks on all workers, including employees, contractors, and consultants; background checks for resources who have privileged access should be performed with repetition. Verify that the background check is appropriately comprehensive and reliable.

11.0 Threat Category: Inherited Risk (Extended Supplier Chain)

11.1 SCENARIO: SUB-AGENCY FAILURE TO UPDATE EQUIPMENT

11.1.1 Background

A Sub-Agency hadn't upgraded their hardware supporting their network routers, switches and hubs for greater than five years. As a result, this agency was unable to receive software updates and therefore putting their agency at a substantial risk and vulnerable position.

11.1.2 Threat Source

These disruptions have taken place across state and local agencies, the private sector, and even at home with personal routers. Threats can come from international unfriendly countries, hackers, etc. Furthermore, the attack can come at any time with persistence and can occur frequently if the condition is not fixed.

11.1.3 Vulnerability

Because this was a sub-agency on the entire agency's network, all sub-agencies became vulnerable. The software from a supplier is not being maintained to its current version across sub-agencies, which has created a vulnerability.

11.1.4 Threat Event Description

This is a network category threat, as business heads and CFO's must be made aware that cutting budgets from network infrastructure is no longer an option. This is due in large part because of the size and scope of the risk posed to an organization's network infrastructure.

11.1.5 Outcome

The objective of the threat actor can be network disruption, data theft, intellectual property and financial threats.

11.1.6 Organizational Units / Processes Affected

N/A

11.1.7 Potential Mitigating Strategies / SCRM Controls

Require flow-down controls and risk management for all subs to pass to any of their subs. Then require audits or compliance reports and attestations.

11.2 SCENARIO: SUB-AGENCY FAILURE TO UPDATE ENTERPRISE SOFTWARE

11.2.1 Background

Enterprise software from a supplier is not being maintained to its current version across sub-agencies.

11.2.2 Threat Source

This threat is applicable across federal, state & local agencies as well as the private sector. The threats could occur anywhere within the supply chain i.e., OEMs, manufacturers, integrators, third parties, etc.

11.2.3 Vulnerability

Unpatched applications.

11.2.4 Threat Event Description

Software is the threat category. The sample threat mentioned above could be a threat to many agencies who does not maintain supported software thresholds (usually 2 previous versions). Non-updated operating systems are also a threat. Some organizations are still running vulnerable and unsupported versions that were deprecated years ago.

11.2.5 Outcome

Intellectual property, network, and disruption are all applicable. Several cities have already had their networks locked up and threat actors are demanding financial settlement to unlock their network and devices.

11.2.6 Organizational Units / Processes Affected

Depending on the software, it could impact the OEM, the reseller or the integrator. There could be cost implications, the integrity of the company may be questioned etc. Out of date software (no longer supported by the OEM or third parties) places unnecessary risk on the agency. Unsupported software places security vulnerability upon the business and the agency. The threat is applicable at any time and persistent within the infrastructure.

11.2.7 Potential Mitigating Strategies / SCRM Controls

Require supply chain organizations to keep their applications and operating systems up to data and patched within 72 hours of a new patch. Require attestations of compliance. Perform periodic audits.

11.3 SCENARIO: INHERITING RISK FROM NTH PARTY SUPPLIER

11.3.1 Background

During the development of components (software or hardware), sometimes exceptions are taken in test cases deemed *noncritical* to the operation of the subcomponent. These are not necessarily the wrong decisions in the testing process, but the failure is a result of not maintaining this information as the element flows up in the supply chain. This results in a lack of traceability as these elements are integrated into higher level components and eventually end products or systems. Furthermore, this can lead to cascading minor errors resulting in a vulnerability or IP license violation in the final product.

11.3.2 Threat Source

This threat is sourced from known and trusted suppliers. It is not intentionally targeting the end procuring agency, but it manifests at that level in the delivered system. This threat typically manifests as a one-time vulnerability in the form of a bug. It is not specific to only software or firmware, although that is more likely. This is an unintentional threat that results from inheriting acceptable risk decisions made by a supplier further down the chain from the end producer of the final product or service. The deeper into the supply chain is occurs, the more difficult it is to identify in advance.

11.3.3 Vulnerability

Unlike a typical threat actor sourced attack on the supply chain, the inherited risk from a lack of transparency can be very difficult to identify and mitigate in advance. It is an accidental vulnerability that is part of the normal system development life cycle and is a known vulnerability, possibly mitigated through proper internal controls. This information is traced within the SDLC of the sourcing supplier and typically provided in release notes to the procuring entity. The challenge is the compounding effect of numerous separate and distinct test exceptions as the complexity and scale of a system increases.

11.3.4 Threat Event Description

This is an inherited risk as a result of the extended supply chain that is an accepted part of the supplier SDLC. It is possible that the subcomponent, assembly, or software is used in a system for which it was not initially intended. The resulting environmental changes or integration with other pieces results in the threat manifesting into an impactful failure.

11.3.5 Outcome

N/A

11.3.6 Organizational Units / Processes Affected

The lack of traceability as these elements are integrated into higher level components and eventually end products or systems can lead to cascading minor errors resulting in a vulnerability or IP license violation in the final product. The objective is not to perpetuate a threat. It is the result of a common trade off in any engineering process concerning cost, schedule and quality.

11.3.7 Potential Mitigating Strategies / SCRM Controls

Good engineering process will ensure that these decisions are documented, and traceability is provided vertically up the supply chain.

11.4 SCENARIO: MID SUPPLY INSERTION OF COUNTERFEIT PARTS VIA SUPPLIER XYZ TO TRUSTED/VETTED VENDOR

11.4.1 Background

During the supply chain process, it is possible that a third party, or upstream supplier ("Supplier XYZ") providing components (software or hardware) to a trusted vendor within a chain has not been vetted to the same caliber as the trusted vendor itself. This can lead to the opportunity of a threat agent delivering, installing, and inserting counterfeit elements to the trusted vendor.

11.4.2 Threat Source

The threat may be sourced by a variety of stakeholders, including the following:

- Nation state actors;
- Cyber criminals;
- Extended stakeholders utilized via Supplier XYZ; and
- Unvetted stakeholders in the extended supply chain, etc.

11.4.3 Vulnerability

The inherited risk from Supplier XYZ can be difficult to detect because stakeholders within the extended supply chain may be hard to trace and enforce the same level of vetting scrutiny as a trusted vendor will be receiving. This vulnerability is the result of an extended supply chain with an unvetted or poorly vetted supplier that has been accepted by the stakeholders using it.

11.4.4 Threat Event Description

This inherited risk effects the transit and integrity of the trusted supply chain. Supplier XYZ can serve as an incognito vehicle for introduction of hostile elements that the vetted supplier may integrate within a product, or component that may be purchased by consumers. If Supplier XYZ had integrated counterfeit parts wittingly, they could have the ability to affect the reliability of the supply chain, products or exploit consumer data.

11.4.5 Outcome

If intentional, Supplier XYZ's objective may be to negatively impact integrity or availability of products and services provided by the upstream trusted vendor. A secondary objective could be damage to the reputation of the trusted vendor. It is possible that Supplier XYZ's objective is not intentional damage but is the result of poor vendor risk management practices.

11.4.6 Organizational Units / Processes Affected

This threat affects hardware and software components within the supply chain. The threat described above, is an inherited risk due to the accepted trust of an extended supply chain member that has not been vetted and trusted by the end buyer. This can lead to insertion of counterfeit products, as well as tampering of a legitimate and integral supply chain.

11.4.7 Potential Mitigating Strategies / SCRM Controls

This threat will persist until Supplier XYZ is identified as the source of the counterfeit materials and removed.

12.0 Threat Category: Economic

12.1 SCENARIO: FINANCIAL STRENGTH OF THE SUPPLIER

12.1.1 Background

Each company is different in capability to respond to financial problems. This depends on a number of factors; including personnel, size, scope of the company, access to capital, and even geographic location. At any point in time, this capability can change.

12.1.2 Threat Source

There is significant overhead in maintaining a secure operational environment within a business enterprise. Some firms operating on razor thin margins, or startups struggling to make a profit will be tempted to cut corners or accept risks that can open up attack vectors to a threat.

12.1.3 Vulnerability

The vulnerability in the scenario was created by not spending funds on using protective software.

12.1.4 Threat Event Description

A company struggling to survive under heavy financial stress just to meet payroll may cut IT staff, stop using protective software, or even share protected files or data with an unauthorized buyer just to stay afloat.

12.1.5 Outcome

These potentially bad results are predicated on weakness in financial strengths of a supplier. Unpredictable or surge orders or customers shifting to a new supplier can cause a company to rebalance to match income with expenses.

12.1.6 Organizational Units / Processes Affected

N/A

12.1.7 Potential Mitigating Strategies / SCRM Controls

Understanding the financial position of your suppliers can help deciding on the need for changes, mitigation strategies, or discussions on how you can help or advise suppliers on improving their operations. Reviewing financial reports from public companies, looking at reports from organizations like Dun & Bradstreet, or having a one on one personal discussions and reviews can all help. A close personal relationship with suppliers will also help mitigate risk.

12.2 SCENARIO: INFORMATION ASYMMETRIES

12.2.1 Background

There will always be a difference between what the supplier knows and what the customer knows. Even for customers, who have people collocated with suppliers, this difference of insights or information can cause decision making that will open up potential threat vectors.

12.2.2 Threat Source

The problem from different knowledge or understanding of a supplier's financial status or economic conditions in the marketplace can create assumptions that everything is going fine, when in fact they aren't.

12.2.3 Vulnerability

Lack of oversight from the customer's perspective - built into contracts with the supplier.

12.2.4 Threat Event Description

The supplier is not following the processes or procedures in securing the product from either physical compromise or digital security of the design. The customer is not aware of their lack of compliance.

12.2.5 Outcome

The lack of information or the partial gathering of information can cause problems from the customer making assumptions that things are proceeding on plan and with approved and documented processes, but when the supplier knows that these efforts are not being maintained.

12.2.6 Organizational Units / Processes Affected

N/A

12.2.7 Potential Mitigating Strategies / SCRM Controls

Place people at the site of a suppliers' production or assembly to monitor or validate. This will incur additional costs but is a control step that reduces or mitigates risk in supply chin compromise.

12.3 SCENARIO: OWNERSHIP CHANGE

12.3.1 Background

Ownership of a supplier can change hands at any time. New investors will be brought into a small business or start up. Successful businesses will be acquired or merged with larger or equal size businesses. If the ownership change involves foreign entities, this can be problematic to the information security of the company.

12.3.2 Threat Source

Large amounts of cash generated by a successful business requires reinvestment. Letting cash sit around unproductively is not usually a smart way to grow a company. Often cash accumulation is used to acquire companies in vertical or horizontal markets.

12.3.3 Vulnerability

Lack of oversight from the customer's perspective - built into contracts with the supplier.

12.3.4 Threat Event Description

A large Chinese firm has successful been a supplier to numerous companies across the globe. This firm targets a U.S. firm in the same market that is considered a competitor for acquisition. This allows for horizontal integration at the same time as a reduction in global competition.

12.3.5 Outcome

The acquisition of firms that control a majority of the market can be considered an anti-trust violation in many countries. This concept or legal restriction does not apply worldwide. Firms that are controlled, subsidized or financially supported by governments can have an unfair advantage in the marketplace.

12.3.6 Organizational Units / Processes Affected

N/A

12.3.7 Potential Mitigating Strategies / SCRM Controls

The U.S. government should protect U.S. firms undergoing unfair competition. CFIUS should restrict sales of U.S. firms to foreign firms, where the acquisition would create a risk to the supply chain or a transfer of control of a critical market to oversight by a hostile of unfriendly government.

12.4 SCENARIO: COST VOLATILITY

12.4.1 Background

Outside of the suppliers' control, there can be governmental or economic drivers that will affect the cost of a specific product. While minor price increases or drops are usually accounted for in the markup of products at each stage of the supply chain, successful companies still have challenges when monetary policy (value of the local currency) is less than stable or when market related events occur (i.e. tariffs are employed for political purposes or economic downturn causes businesses to react differently). This can be quite problematic for multiple parts of the supply chain. This is especially true for ICT supply chain which works on thin margins to start with.

12.4.2 Threat Source

The value of currency and politically volatile events can have serious implications on taxes (tariffs) and the true cost of trade across multiple currencies. One way around this is to diversify your supply chain sources to develop contingencies should volatility arise on supply costs. This is part of a good supply chain risk management strategy.

12.4.3 Vulnerability

N/A

12.4.4 Threat Event Description

The Chinese government is suspected of limiting output of the rare earth element, neodymium, to a number of external suppliers. Neodymium is essential in the manufacturing of permanent magnets. Various countries have various amounts of Neodymium stockpiled for multiple industries. Neodymium has fluctuated extensively in price over the past 5 years and affects the pricing of hard drives and other electronics that much of the world counts on from Vietnam, China and other Asian countries. Since China has over 90 percent of the earth's known quantity of Neodymium, at various times, they have taken political actions that cause dramatic volatility in the price and amount of Neodymium available worldwide.

12.4.5 Outcome

The ability for U.S. or other countries' to invest in Chinese mines has been very limited to non-existent by the Chinese government. Chinese firms have sought to invest in the companies that use the rare earths to expand their ability to control more of the technology marketplace. These firms are backed by the Chinese government and they're usually state owned or managed companies. They can use rare earths to affect prices outside the country (initiate volatility) and ensure supply and low cost for state owned companies (inside China) to affect the volatility, price and supply chains for various products.

12.4.6 Organizational Units / Processes Affected

N/A

12.4.7 Potential Mitigating Strategies / SCRM Controls

U.S. companies need to work with businesses and countries outside of China to diversify their supply chains and lower supply chain risks. R&D needs to consider possible replacements for rare earths that are politicized. Supply chains can, likely at additional cost, work to obtain and seek out rare earths from other sources. Additionally, some rare earths can be obtained at a lower price if they are provided before they're separated but will incur some cost for the separation of the rare earths from their source. The goal from these mitigations will likely yield a diversified source of products that can obtained needed Neodymium at a more stable price structure than competitors. Competitors will likely have to add margin to deal with the multiple variables that will add excess market costs to their supply chain.

13.0 Threat Category: Legal

13.1 SCENARIO: LAWS THAT HARM OR UNDERMINE AMERICAN ECONOMIC INTERESTS

13.1.1 Background

Under U.S. federal and (most) state law, trade secrets have protected status, which helps to enable the cyber supply chain to flourish. This same type of legal protections does not exist in every country where a company – or entities in the company's supply chain - is located or transacts business.

"China has implemented laws, policies, and practices and has taken actions related to intellectual property, innovation, and technology that may encourage or require the transfer of American technology and intellectual property to enterprises in China or that may otherwise negatively affect American economic interests. These laws, policies, practices, and actions may inhibit United States exports, deprive United States citizens of fair remuneration for their innovations, divert American jobs to workers in China, contribute to our trade deficit with China, and otherwise undermine American manufacturing, services, and innovation." Excerpt from Presidential Memo to the U.S. Trade Representative, 2017.

13.1.2 Threat Source

State and quasi-state threat actors refers to hostile governments that want to disrupt American cyber supply chains for strategic or tactical advantage. It is also a reference to any governing authority that de facto acts as a state. Lack of diplomatic recognition as a state does not affect the actor's ability to operate as a supply chain threat. These actors are defined by their strategic or tactical reasons for wanting to disrupt American cyber supply chains and their ability to employ state or state-like powers to achieve that end, not the formalities of diplomacy, such as state-owned enterprises—who would look to steal American intellectual property. State-owned enterprises and similar quasi-state actors around the world seek advantage in the marketplace and in the operation of whatever end they are tasked by their associated government.

Quasi-state actors are largely synonymous with state-owned enterprises. These are businesses or organizations that operate independently of any government, at least on paper, but are influenced by a government to such a degree that the organization is either effectively owned or controlled by it. These quasi-state actors are different from state actors in that they have some private function—usually a market function—but nor can they escape government-given public functions. These public functions may include manufacturing of military equipment, maximizing employment, or dominating a sector seen as strategic to the state-actor's national interests.

13.1.3 Vulnerability

Businesses operating in or desiring to sell their goods to nation states, such as China, may be subject to legal requirements that could result in the loss of their intellectual property or the undermining of their market share.

13.1.4 Threat Event Description

The state actor opts against enforcing (or not having) intellectual property protections and forces technology transfers. This allows a state actor to unleash non-state third parties and quasi-state actors to pursue their objectives to steal intellectual property without domestic legal consequence. A more overt method of obtaining IP is via forced technology transfers (a government-mandated transfer of intellectual property from the original owner to some other entity).

13.1.5 Outcome

This fundamentally harms trade secret protections. Further, once stolen intellectual property is in the wild and with few legal protections and remedies, it can result in counterfeit parts and sabotage that may cause disruptions in the cyber supply chain, denial of end products, and failure of the end products.

13.1.6 Organizational Units / Processes Affected

N/A

13.1.7 Potential Mitigating Strategies / SCRM Controls

There are limited mitigation options. Suppliers should be aware of the legal requirements of the countries in which they operate, do business and consumers should be aware of which of their suppliers may be subject to these onerous laws.

13.2 SCENARIO: LEGAL JURISDICTION-RELATED THREATS

13.2.1 Background

Company A relies upon a foreign-based manufacturer to produce a key component of its product. The country the manufacturer is located is known for government corruption and weak oversight of its domestic businesses

13.2.2 Threat Source

Supply chain entity is threat actor: Entities within the global supply chain can intentionally or unintentionally introduce threats into an end product deliverable. Actors may have nefarious intent, be profit-motivated, or simply negligent.

13.2.3 Vulnerability

A threat actor has the opportunity to engage in nefarious behavior in a jurisdiction unlikely to punish or deter such behavior. The problem of security become more complex and therefore more expensive.

13.2.4 Threat Event Description

The manufacturer uses inferior material to produce the components for Company A while charging Company A for the costs of the more expensive, specified material and falsifying its financial records. Manufacturing company managers pocket the savings in costs they generate from using cheaper material. This introduces a weakness in the product that cannot be readily identified but will cause the component and to fail prematurely.

13.2.5 Outcome

Poor security from entities within a supply chain has potentially devastating implications for delivery of an end product. When the supply extends across multiple countries, differing legal jurisdictions introduce multiplied and varied threat opportunities.

13.2.6 Organizational Units / Processes Affected

N/A

13.2.7 Potential Mitigating Strategies / SCRM Controls

Businesses offering goods and services should carefully vet the businesses within their own supply chains to ensure that the deliverables they provide to their customers will appropriately perform and be trustworthy. In this scenario, Company A may want to consider controls such as third party auditing or monitoring, oversight of manufacturing processing by on-site Company A personnel, or a product testing program to ensure the components delivered are conformant to specifications. Acquirers' of Company A's products should seek to understand how Company A ensures the quality and trustworthiness of its products- especially if the product is intended to be used for a critical mission or business purpose.

13.3 SCENARIO: LEGAL COSTS THAT WEAKEN THE FINANCIAL VIABILITY OF A COMPANY

13.3.1 Background

A medium sized business provides a niche service to a Government customer that is critical to the Government customer's mission. There are only a handful of other businesses in the marketplace that can provide this service.

13.3.2 Threat Source

N/A

13.3.3 Vulnerability

The medium sized business has limited cash reserves and has made a business decision to reinvest a majority of its profits to grow the business through marketing and an expansion of its sales force. While the business has made some investments in new technology and has a small team that manages the IT, there are no dedicated personnel focused on IT security and only basic security protections are in place.

13.3.4 Threat Event Description

One of the IT personnel finds evidence that one of the systems may have been breached. This system contains employee related data that is confidential in nature. After hiring a security firm, the evidence was insufficient to be able to determine whether a breach actually occurred and if so, whether data were accessed. The business' legal firm advises that all company personnel must be notified and offered identify protection services for no less than one year. The business is also advised that they must notify their government customer, per their contract terms and conditions. The company fears their contract may not be renewed. Legal costs are significant.

13.3.5 Outcome

According to a study at Champlain College, sixty percent of Small and Medium-sized Businesses (SMBs) will go out of business within six months after a data breach. The reasons for this are not likely to be exclusively legal, but the legal costs associated with a data breach are certainly significant for SMB suppliers in the cyber supply chain and there is the potential for resultant business closures.

13.3.6 Organizational Units / Processes Affected

N/A

13.3.7 Potential Mitigating Strategies / SCRM Controls

It is important to consider to what extent unplanned for legal costs may undermine the financial viability of a small or medium sized company. If this business provides a critical service or product, it would be prudent to investigate the strength of the company's financial resources prior to engaging in a contractual relationship or ensure that there are readily available alternative sources of supply that could be quickly acquired should the firm find itself in unanticipated financial trouble and go out of business or fail to perform satisfactorily due to constrained resources.

This scenario describes legal costs that arise out of a data breach. Other sources of legal costs can include: settlements and pending litigation against a business, fines and penalties levied against the company, and contractual-related liabilities arising from actions such a termination for cause or stemming from threats introduced by extended supply chain partners or sub-tier subcontractors.

14.0 Threat Category: External End-to-End Supply Chain

14.1 SCENARIO: NATURAL DISASTERS CAUSING SUPPLY CHAIN DISRUPTIONS

14.1.1 Background

External events including natural disasters can have a large impact on the end to end supply chain ranging from destruction of manufacturing facilities, the ability to receive production materials to the ability of workers to get to work, to the ability to distribute final products to mention only a few. Depending on the size and scope of the event, the disruption to the end-to-end supply chain can have multiple impacts.

14.1.2 Threat Source

Natural disasters can have a severe impact on our global economy. According to Aon Benfield's 2016 Global Climate Catastrophe Report, the world saw $210 billion in economic losses because of 315 separate natural disasters. That's 21 percent above the 16-year average of $174 billion. In 2017, Hurricane Harvey victims saw over 178,000 homes lost, $669 million in damages of public property, around a quarter million vehicle losses, $200 million in Texas crop in livestock losses. Additionally, businesses saw significant and expensive losses due to flooding, electrical outage, and employees' inability to get to work, all causing temporary disruption of the flow of goods and services. But the impacts of natural disasters reach far beyond the local damages of affected areas. When these natural events happen, many businesses find their supply chains greatly impacted.

The Tohoku Earthquake and Tsunami in Japan and the Thailand Floods in 2011 are both examples of natural disasters that had expanded indirect economic effect. Both disasters caused severe disruption to global technology supply chains. After the Thai floods, there was a global shortage of computer hard drives that sent consumer prices skyrocketing until factories were able to get back up and running. When the 2011 tsunami struck, several major until business operations were restored to normal. Car manufacturers were forced to shut down production at factories throughout Europe and the U.S. due to a lack of available parts from factories in Japan, setting off a supply chain reaction that impacted multiple suppliers of parts throughout the wider global economy.

14.1.3 Vulnerability

N/A

14.1.4 Threat Event Description

A category 5 hurricane has hit in Savanah, GA, and has moved up the east coast and inland in northern VA before becoming a tropical storm. The hurricane damaged or destroyed ports from Savanah, GA to Norfolk VA while also destroying roads and bridges. Critical infrastructure impacts were also wide spread, specifically impacts to power and communications.

14.1.5 Outcome

The ever-growing reach of global supply chains exposes these networks to serious vulnerabilities. In this scenario, a medium sized manufacturing company has been impacted in several ways. First there are impacts to getting materials into the manufacturing plant and the ability to distribute and finished products leading to financial harm, such as unrecoverable loss of revenue or accounts receivable, as well as contractual fines and penalties; the inability to provide effective customer relations and regulatory reporting; and damage to relationships, brand or corporate reputation and confidence.

14.1.6 Organizational Units / Processes Affected

N/A

14.1.7 Potential Mitigating Strategies / SCRM Controls

Following established steps to identify potential risks to the supply chain and plan for business interruptions is critical for a company’s survival in times of natural disasters.

The first step is to complete a Business Impact Analysis (BIA). This analysis provides a complete understanding of the business and its supply chain, allowing organizations to identify exposures and potential mitigation measures. It helps identify the most feasible and cost-effective strategies and solutions for business continuity and disaster recovery. In addition, reviewing insurance policies as they relate to business interruption enables companies to detect any areas requiring additional coverage.

Following the BIA, the second step is disaster recovery preparation. Based on the results of the impact analysis, this exercise finds critical business functions, resources and methods; reveals business unit, supplier and customer interdependencies; further identifies potential threats and exposures; and helps users ascertain potential losses and impacts, should a disaster occur. The process involves documenting recovery time objectives, IT interdependencies and manual procedures; evaluating existing recovery capabilities; and creating effective mitigation measures, including the recovery plan documenting who to call, where to go and who will do what in the event of a disaster. It also identifies which tasks must be considered mission-critical. The plan sets a schedule for periodic backups of all electronic and hard-copy documentation, which should be stored in an alternate location.

Focus on creating a stable, yet flexible, supply chain. Diversifying suppliers and methods of transport wherever possible is an effective strategy. Also consider alternate supplier teams and define roles both internally and externally to enable this emergency supply chain. Backup work locations, redundant IT systems should also be a priority.

The body of the recovery plan should include the following:

- Business assumptions;
- Incident-management team member including critical personnel from all areas of the company resources and recovery assignments;
- Recovery strategy and solution overview;
- Emergency-response procedures;
- Incident-reporting procedures;
- Recovery team notification, mobilization and assembly procedures;
- Detailed recovery procedures;
- Situation-assessment guidelines;
- Emergency contact information of key employees, vendors and customers;
- A summary of mission-critical business functions to be recovered; and
- Detailed procedures for transitioning back to business as usual.

Finally, the third step in the process is to regularly test the plan. A plan is only as good as its execution. A table top exercise is an effective way to test and validate the plan by ensuring all internal and external team members are familiar with their roles and responsibilities. Aside from assisting team members practice their roles, develop confidence and expertise it can reveal any necessary gaps and needed updates.

14.2 SCENARIO: MAN MADE DISRUPTIONS: SABOTAGE, TERRORISM, CRIME, AND WAR

14.2.1 Background

Man-made events such as fire, product defects, cyber-attacks, labor and civil unrest, terrorism, utility failure, and piracy are frequent disruptors of supply chains, but typically have a lower severity than natural catastrophes.

14.2.2 Threat Source

The year 2016 saw several man-made disruptions, including the late summer Gap warehouse fire in Fishkill, New York, which destroyed 30 percent of Gap's total warehouse space and disrupted more than 10 percent of Gap's orders. Another example is the Samsung Note cellphone battery recall, which was linked to problems in a battery supplier's supply chain and had far-reaching consequences for the Samsung brand and their customers.

The past few years have seen an increasing prevalence of cyber-attacks. Most of these incidents, such as the high-profile Equifax data breach that involved the personal information of some 143 million Americans, and the Dyn cyber-attack which took down some of the world's most popular websites such as Twitter, Airbnb, and Netflix, do not directly affect supply chains. However, they raise major red flags for supply chain practitioners. It seems that cyber criminals have a growing number of avenues of attack at their disposal, especially given the exponential growth in the number of Internet-enabled devices and cloud-based communications networks.

14.2.3 Vulnerability

N/A

14.2.4 Threat Event Description

The collision of carriers in the waterway ceased operations at the Twin Ports. The collision resulted in one of the vessels taking on water, which caused the vessel to capsize dropping the containerized units from the vessel into the waterway, destroying the products in the containerized units

The cargo carriers not affected in the collision sat idle until which time they received direction from the port authorities on how to proceed. The carriers were either directed up the coast to a different port or were instructed to stay put until they could resume operations and accept the cargo at the Twin Ports.

14.2.5 Outcome

The majority of overseas cargo comes from Asia and therefore come into ports on the West Coast. Los Angeles and Long Beach handle over 40 percent of U.S imports from Asia. Due to the heavy cargo traffic, a collision of 2 cargo ships occurred in the waterways halting operations to the Twin Ports in Los Angeles and Long Beach.

14.2.6 Organizational Units / Processes Affected

The collision created a delay in delivery of network components to the U.S. Company. The components could have been destroyed if they were in a containerized unit that fell into the water, or a significant delay could occur if the components were on a ship that was re-routed to a different port due to the port closures at Twin Ports.

The U.S. Company was able to track down their shipment and determined that it was taken to a port in New Jersey and arranged for ground transportation to obtain the shipment and deliver to the U.S. Company.

The U.S. Company missed their committed lead times resulting in a delay in delivering their network equipment to customers. Due to the missed due dates, the U.S. Company was expected to pay liquidated damages that were contractually agreed to with their customers.

14.2.7 Potential Mitigating Strategies / SCRM Controls

To avoid future scenarios such as the one described above, the ports should monitor the traffic 24/7 to avoid congestion of ships when approaching the ports.

Additionally, a protocol should exist amongst ships that if any ship is within .5 miles from another ship, the ships communicate with one another and, based on the protocol, one ship remain idle until the other ship has cleared the port.

14.3 SCENARIO: LABOR ISSUES

14.3.1 Background

An organization has decided to perform a threat scenario analysis of its resource and capacity planning. The scenario will focus on the sensitivity of the business to unforeseen fluctuations in the country's unemployment rate.

14.3.2 Threat Source

GoFast Auto Company is a 1.5 million square foot manufacturing facility that produces 45 million automotive parts per year. The company supplies mainly to after-market retailers but does have some direct contracts with major automotive manufacturers in the United States to produce proprietary parts. There are 35,000 employees, 28,000 of which are directly tied to production and run three full shifts. The production organization is made up of machinists, technicians, inventory control, quality assurance, design engineering, and other occupations ranging in skill and education level.

14.3.3 Vulnerability

N/A

14.3.4 Threat Event Description

The organization has established the following fictitious threat for the analysis exercise:

Two years ago, there had been a lot of political momentum to enable better, higher-paying jobs in manufacturing and other blue-collar jobs. Due to this, a year ago, there were several programs that were funded by the U.S. government to encourage brining jobs back to the U.S. from oversees locations while also increasing wages. After three phases of these programs touching on different industries, the U.S. has seen its unemployment rate drop from 8.5 percent to 3.4 percent.

14.3.5 Outcome

With unemployment at low levels, there has been a lot of job movement, particularly in the manufacturing sector. As a result of this, GoFast has seen attrition at 3x the normal rate. Labor levels have dropped off to the point where the production of some components has had to be delayed or even halted. The reduction in volume produced has directly led to a drop in revenue, and one contract for proprietary parts was terminated. In 6 months, revenues have dropped 13 percent.

GoFast attempted to rectify some of the impact by moving employees into more critical roles, but generally, the training time for a major role change is approximately 4 months. Additionally, GoFast has reached out to several consulting and staffing firms, but there are two issues with this. One is the personnel from these outlets would take even longer (6-8 months) to fully ramp up as they are brand new to the company, and two is even the staffing firms are having trouble attracting skilled talent.

14.3.6 Organizational Units / Processes Affected

N/A

14.3.7 Potential Mitigating Strategies / SCRM Controls

- Institute a standard rotation or cross-training process for all, or at least employees in critical roles;
- Offer more competitive packages for skilled people looking for new opportunities in the marketplace;
- Entice more employees to stay with perks, including wage increases, benefits, time off, educational and training opportunities, flexible hours, or other options that make sense for employee and employer;
- Simplify processes or improve related training and documentation to reduce transition or onboarding time for folks new to an area; and
- Work with local trade schools and universities to develop talent with specific skills that are currently lacking in the workforce.

14.4 SCENARIO: INFLUENCE OR CONTROL BY FOREIGN GOVERNMENTS OVER SUPPLIERS

14.4.1 Background

An organization has decided to perform a threat scenario analysis of its Printed Circuit Board (PCB) suppliers. The scenario will focus on the sensitivity of the business to unforeseen fluctuations in component costs.

14.4.2 Threat Source

Apex PC Corporation designs, assembles, and ships 3.5 million personal computers per year. It has a global footprint both in terms of customer and supply bases. Five years ago, in an effort to reduce the cost of goods sold, Apex shifted a majority of its PCB procurement to Southeast Asia. In an effort to not be single sourced, Apex finalized agreements with five different suppliers within the country and has enjoyed a positive partnership with each during this time.

14.4.3 Vulnerability

N/A

14.4.4 Threat Event Description

The organization has established the following fictitious threat for the analysis exercise:

Last year, the country where Apex does most of their PCB business has seen a new regime take over the government. This regime has been more focused on improving finances and business environment within the country, allowing larger firms who set up headquarters and other major centers within country advantages to more easily and cost-efficiently do business with suppliers within the same region.

In February of 2019, this now-corrupt regime has passed new legislation that establishes an additional 20 percent tax on all electronic components and goods sold outside of the country. This new law was to take effect on June 1, 2019.

At the time the new law was announced, the current Apex inventory of PCBs was about 10 percent of yearly demand, which was the typical level of inventory they were comfortable with. Before June, Apex reached out to all five suppliers to order additional materials, but there was quickly a shortage due to higher demand from many foreign customers of these products. By June 1, the day the new tax law took effect, Apex was up to an inventory level of up to 15 percent of yearly demand.

14.4.5 Outcome

Between February and June, Apex also looked to partner with new suppliers, but there were several issues found with this. For one, of the 10 new suppliers Apex reached out to, the lead time for ramping up to desired demand was anywhere from 6 months to 18 months. This would include work on Apex's end, to include testing samples of the supplier PCBs and working out logistics details, to supplier-side activities such as procurement of raw materials and acquisition of additional personnel, production space, etc. necessary to meet the new demand.

The second issue is due to the current contracts with all five current suppliers in Southeast Asia, there were minimum demand requirements, meaning Apex was committed to purchasing a minimum of 100,000 PCB's per month for the duration of the contracts (which ranged anywhere from 3 months to 24 months remaining). This would mean Apex could not easily avoid the cost implications of this new tax.

Could Apex absorb the cost of the PCBs? With a 20 percent cost increase, this eroded the margins of a PC from 13.5 percent down to 4.5 percent, on average. For some of the lower margin Apex offerings, it would likely mean discontinuing the line and using these now more expensive PCB's on higher-end models that could carry more margin.

14.4.6 Organizational Units / Processes Affected

N/A

14.4.7 Potential Mitigating Strategies / SCRM Controls

- Diversify suppliers not just by immediate location, but country, region and other factors;
- Build cost implications into supplier contracts, making it easier to walk away from suppliers when costs rise too high (whether its fault of the supplier or not);
- Adjust desired inventory levels to better account for unexpected shortage of demand at critical times; and
- Employ more resources in countries or regions of key suppliers in hopes of receiving advanced Intel of new legislature that may negatively affect business.

14.5 SCENARIO: MALICIOUS SUPPLIER INSERTS HOSTILE CONTENT

14.5.1 Background

A software supplier, NMT-Com provides network management infrastructure for numerous global companies. Recently, several customers have complained about products that have ended up failing certain security scans upon receipt, although the majority of customers have had no reported issues.

14.5.2 Threat Source

NMT-Com has software developers around the world, with a dozen different code compiler locations, at their primary development centers. Software packages and libraries are uploaded for review and security scanning and then stored where they can be utilized by developers within the region; customer support is handled by the regional center that supplies the software load.

Product packages are intended to be consistent across customers, for easier support, patching and development. Release testing is done on a periodic basis in the development cycle at each center.

14.5.3 Vulnerability

According to the scenario presented, since NMT-Com has a dozen difference code compiler locations, there is the potential for a bug to be inserted into the code, thus creating a vulnerability.

14.5.4 Threat Event Description

A malicious supplier employee inserts hostile content at the product or component manufacturing or software compilation stage to affect supplier products or components delivered to a targeted subset of downstream customers.

14.5.5 Outcome

Due to the disconnect between the process of where software is scanned and where it is compiled and released, there is a potential for insertion of malicious software. There is an assumption of trust at the compiler locations and no re-scanning is done, except on the full release on a periodic basis (rather than every time it is changed and before it is signed.

This could leave customers of the supplier open to backdoor exploits, software injection attacks, data manipulation, data exfiltration or any number of attacks possible if the very code itself is compromised.

14.5.6 Organizational Units / Processes Affected

N/A

14.5.7 Potential Mitigating Strategies / SCRM Controls

- The supplier should implement, monitor and audit a comprehensive security assurance framework as part of their software development process;
- All software should be compiled in trusted locations, such as where it is also verified, scanned and signed. This would also serve as a logical central distribution point. Whenever software is changed and re-compiled, there could be a potential for injection of malicious code; thus, security scanning should be performed on each of these loads; and
- Static and dynamic code inspection is commonly used to verify the security and integrity of software. Static testing involves checking the code from an internal standpoint, executing code paths and routines to ensure they are operating as expected. Dynamic (aka black box) testing involves mimicking attacker behavior from the outside, detecting known vulnerabilities and simulating theoretical ones to determine if the product is vulnerable to different kinds of exploits.
- Consider keeping code repositories and compiling functions in the cloud.

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise. This report is TLP: WHITE: Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp.

DHS POINT OF CONTACT

National Risk Management Center
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
NRMC@hq.dhs.gov
For more information about NRMC, visit www.cisa.gov/national-risk-management

PDM20003